REPORT on

The 2nd EU-US Summit Workshop on Cyber Trust: System Dependability and Security

Workshop held in Urbana-Champaign, Illinois, USA 26-27 April 2007

Workshop organised and hosted by the Information Trust Institute, University of Illinois in close co-operation with the US National Science Foundation (NSF), the US Department of Homeland Security (DHS), Waterford Institute of Technology (WIT) and the Unit F5 "Security" of European Commission's Directorate General Information Society and Media.

Author: Jim Clarke,

Waterford Institute of Technology, Ireland

Contributors:
William Sanders, University of Illinois, USA
Molly Tracey, University of Illinois, USA
Neeraj Suri, TU Darmstadt, Germany
Paul Barford, University of Wisconsin, USA
Michael Bailey, University of Michigan, USA
Roberto Baldoni, Università di Roma, Italy
David Nicol, University of Illinois, USA
Michel Riguidel, ENST, France
Jody Westby, Global Cyber Risk LLC, USA
Workshop Organising committee, Workshop attendees.


Table of contents


NATIONAL SCIENCE FOUNDATION
NSF


European Commission
Information Society and Media


Homeland Security

Executive Summary

The second EU-US research workshop on "Cyber Trust: System Dependability and Security" was held in Illinois, USA on April 26th and 27th, 2007. It was attended by 40 delegates from the EU and the US, along with a few representatives from Canada, Australia and Japan. The event was organised and hosted by the University of Illinois in close co-operation with the US National Science Foundation (NSF), the US Department of Homeland Security (DHS) and the "Security" unit of the European Commission's Directorate General Information Society and Media. The workshop aimed to ensure progressive continuity of the consensus building achieved at the first workshop on the same subject held in November 2006 in Dublin, Ireland. The guiding principle was to identify and develop further those research areas that require and will benefit from international collaboration, while examining the structures and mechanisms that could potentially enable and fund the proposed work.

The workshop was structured around two main technical themes:

(1) "Architectures, Protocols and Environments for Trust, Security and Dependability (TSD) of future Polymorphic Networked ICT Systems";

(2) "TSD Attributes and Mechanisms for future Distributed Services and Content, future Overlay Networks and Applications".

A transversal topic was also introduced across these two technical themes covering "Test beds, data sets, and models for quantification, evaluation and validation".

At the workshop, there was a broad agreement that the current EU-US cooperation was necessary and should be further elaborated. The workshop also permitted to draft a joint list of research topics relevant for international cooperation and stimulate further discussion on how this could be implemented. The main workshop conclusions are summarised below:

(1) ***Session 1: Architectures, Protocols and Environments for TSD of future Polymorphic Networked ICT Systems***

The session focussed particularly on the security and dependability of future large polymorphic, networked, multi-formed and interdependent ICT systems. Examples of such systems include: the future internet; the internet of “things”; GPS/Galileo; future wireless and mobile systems, RFID and sensor networks (Post IP, Post 3G); mixed mode environments consisting of diverse computing, communication and storage capacities; service-centric, adaptive, heterogeneous and scale-free ambient environments; etc. It was stressed that present security mechanisms based on boundaries and firewall protection mechanisms do not scale up to address the security and dependability of such future complex systems. There is thus a need for joint research in developing autonomic, evolvable and adaptive security mechanisms and policies and new cognitive techniques and semantic models for managing the complexity and interdependencies of such ambient systems and their interaction with users. Security and cryptographic mechanisms and protocols must also be scaled down in order to be inserted in small devices having scarce resources, while at the same time ensuring privacy protection.

(2) ***Session 2: TSD Attributes and Mechanisms for future Distributed Services and Content, future Overlay Networks and Applications***

The session addressed the security of applications and services and the protection of data and software systems; the security in specific service application areas requiring collaboration at global scale like financial, health and critical information infrastructures; and, the security in dynamic service coalitions, including the provision of dynamic service virtualisation in polymorphic environments and the trustworthy delivery of atomic or composite services to end users through a contract that provides them with some security guarantees. International collaboration is needed because such service

coalitions have elements of dynamicity and trust and require the establishment of contracts over unknown and global paths. Such services need to be trustworthy and accountable while they traverse networks spanning over different countries and administrative domains that obey different regulations and policies. These policies have to be interoperable and dialogue and negotiate in real time.

Test-beds, data sets, and models for quantification (metrics), evaluation (techniques) and validation (processes)

The following topics were debated in both the above sessions:

Consumer issues: They include the need to build mechanisms that guarantee privacy, traceability, anonymisation and use of pseudonyms of the legitimate users, while at the same time they permit to locate, track and trace malevolent users at individual, group or organization levels. A new security paradigm needs to be defined that strikes a reasonable balance between a 'Big Brother Society' and a confidence building, privacy and ethics protecting society. Establishing society's confidence in the new digital world would require creating a palpable security environment that enables citizens to control the type and level of protection associated with the digital goods and services they have access to. It would also require developing trust, security and dependability technologies that are unobtrusively and transparently integrated in daily life and not becoming a source of potential problems and nuisance as often perceived today.

Emerging Global Risks: Digital systems evolve, but the threats and types of attacks also change continuously. There is, thus, a need to permanently survey and identify new attacks, to monitor potential network and service vulnerabilities and to look for new emerging risks. Examples of such risks at the global level include: excessive disclosure of private information, bullying, identity theft and squatting and predators masquerading.

International Test-beds and Datasets: Ways to interconnect test-beds should be explored, including the connection of test-beds that were developed as standalone by the different countries. Such test-beds would permit to share data sets and carry out validation in a co-ordinated manner, internationally. Cooperation can be established on various levels: means and results, approaches, infrastructures, software and data. The problem is how to federate such test-beds, taking into account cross-testing, mobility aspects and security policies as users move in and out of different environments. Additional problems to address for enabling the sharing and exchange of data and information relate to the intellectual property, interoperable data formats in repositories, the "diluted glory" factor, the confidentiality or the reproducibility of experiments. Two specific examples of future test-beds discussed were a test-bed on international application and software services that could be built on top of GENI with a number of application-level experiments and a test-bed for wireless or sensor networks.

Mechanisms for International Collaboration: Participants also discussed mechanisms that EU and US funding agencies could make available to assist the continued international collaboration. These included the establishment of a co-ordination type project that could act as catalyst to facilitate, drive and set up future activities in a systematic fashion. Ideas for additional international projects included dynamic service coalitions, privacy, and legal considerations for global cyber-security involving all relevant stakeholders (technologists from academia and industry, policy makers, legal, consumers). A number of realistic cooperation mechanisms based upon existing programmes in each country were also presented by representatives of the European Commission, NSF and DHS. The Japan Science and Technology Agency and Australian NICTA have indicated a willingness to run a parallel programme that could work alongside the EU and US efforts.

1. Introduction: Workshop Objectives, Themes and Format

The second EU-US workshop on Cyber Trust: System Dependability and Security was designed to build upon the results of the first workshop held in Dublin, Ireland, 15-16 November 2006. The first workshop was organised around six panel sessions, as shown in Figure 1. The full workshop report is found at: http://www.securitytaskforce.org/images/stories/eu_us_cyber_summit_report.pdf).

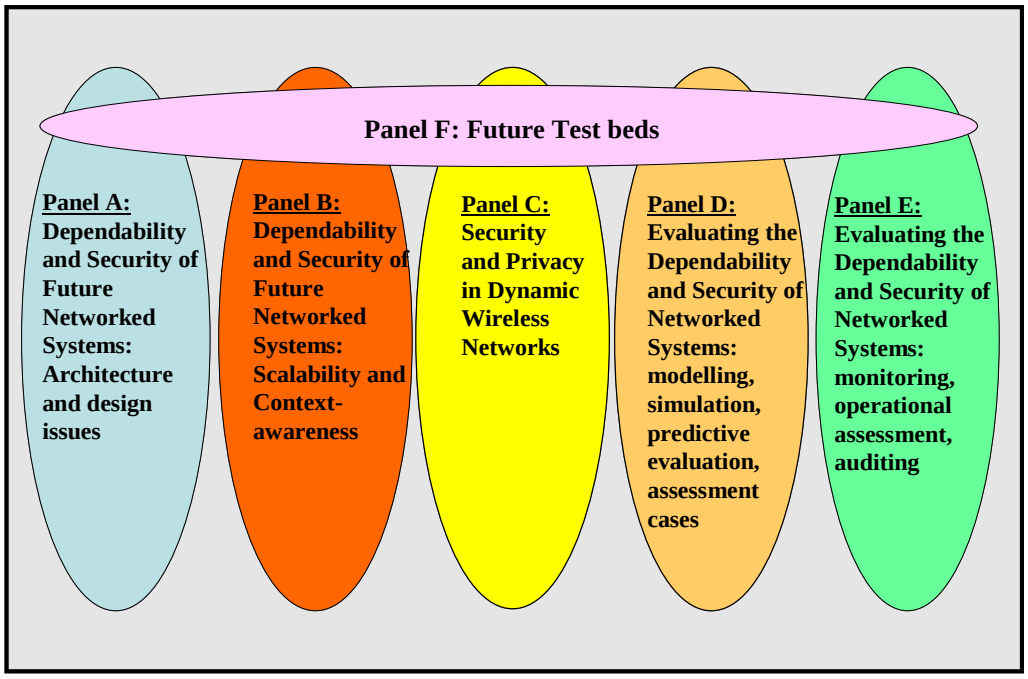


Figure 1: EU/US Summit Series – Workshop 1 Panel sessions

For the second workshop, the Organising committee decided to focus the themes based upon the outcomes from the first workshop as shown in Figure 2. The working sessions of Workshop 2 were, thus, broken into two parallel sessions. Both were incorporating a common theme towards potential shared resources such as test beds, data sets, and models for quantification, evaluation and validation. The themes were thus defined as follows:

Theme 1: Architectures, Protocols and Environments for TSD of future Polymorphic Networked ICT Systems

Issues to be addressed under this theme may include the elaboration of the TSD specifications for the design of the architectures, protocols and environments of future polymorphic networked ICT systems. Examples include: the future internet, the internet of "things"[1], future wireless and mobile systems and sensor networks (Post IP, Post 3G), mixed mode environments (MME) consisting of diverse computing, communication & storage capacities, and service centric (adaptive, heterogeneous, scale-free) ambient environments, among others. These systems will be characterized with heterogeneous technologies and new approaches reconciling fixed and wireless systems, pervasiveness and mobility.

Designing for TSD and QoS for both large systems and small scale devices that have scarce resources is a fundamental requirement for future polymorphic networked systems, MMEs and Critical Infrastructure overlays. This constitutes the base "system/service model basis."

[1] www.itu.int/internetofthings/

Theme 2: TSD Attributes and Mechanisms for future Distributed Services and Content, future Overlay Networks and Applications

Following the design of "system architectures" addressing TSD drivers, the consequent thrust is on development of attributes and mechanisms needed to provide & enhance (on demand and at run-time), the desired security and dependability within the MME & across multiple domains, whether fixed or mobile.

In addition to securing the "system," there is a need to look at securing the applications and services which operate across these future polymorphic networked systems.

(1) Attributes (requirements, specifications, etc.) to provide the required dependability, security, and more broadly, trust, needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies across multiple domains.

(2) Related to the above, are a number of associated mechanisms to improve TSD such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions.

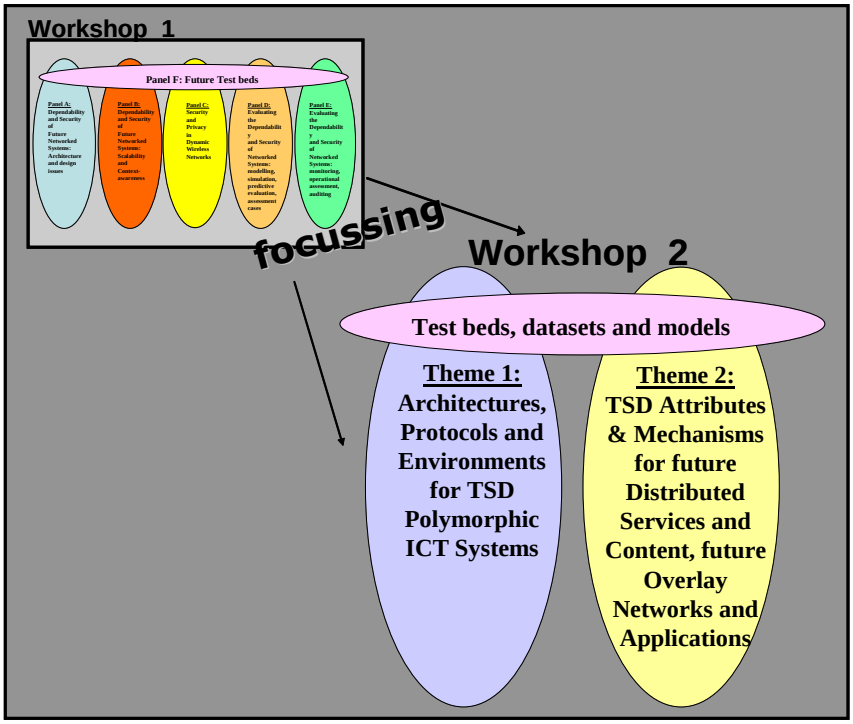


Figure 2: EU/US Summit Series – Workshop 2 Panel sessions

Common issue for both Themes: Test beds, data sets, and models for quantification (metrics), evaluation (techniques) and validation (processes)

In order to be adopted, the infrastructure, mechanisms, and policies developed as part of the first two themes need to be shown to achieve stated dependability, security, and trust requirements. Such evidence must be credible, quantifiable, and make a clear case for a proposed approach. This evidence will come from a variety of sources: test beds, analysis of datasets, and models.

Within this horizontal theme, the workshop explored ways of validating proposed solutions relating to Themes 1 and 2, focusing on the development of resources that can be shared by the EU-US-Japan-Australian communities. These resources will include 1) collaborative test beds for explicitly "quantifying,

assessing and validating" (a) design for TSD in future system architectures and environments and (b) the proposed attributes and mechanisms of new distributed services & content, new overlay networks & applications, 2) creation of datasets that can be used to evaluate proposed approaches, and 3) models that provide understanding of the dependability, security, and trust of proposed systems under varying environmental conditions.

Format of the working sessions

Before the workshop, the Organising committee, in collaboration with the session Chairs, drafted a number of questions that were sent to the workshop participants for best preparing themselves for the working sessions (See Annex B for more details). These would be oriented towards results oriented discussions and brainstorming with a minimum of formal presentations.
It was agreed also that the output of these sessions would be structured around the following issues:

- A prioritized list of the technical directions that should be pursued in each of the theme areas. The list should include the common issues of test beds, data sets, and validation.
- Justification for pursuing each direction, a) in terms of its intrinsic technical merit, b) why it should be done now (what is the urgency), and c) why it is particularly relevant for International collaboration: did it meet the criteria for International collaboration (see the International collaboration criteria in Annex E).
- What are mechanisms that should be set up on the EU and US side in order to facilitate the recommended directions and collaborations.

The remainder of this workshop report is organised as follows:

Section 2 presents the final reports from the chairs and rapporteurs of the sessions. Section 3 outlines the final conclusions. Annex A presents the organising and steering committee members of this workshop. Annex B contains all the requested inputs from the participants. The workshop agenda is outlined in Annex C and the full list of participants is outlined in Annex D. Annex E contains the definition of International collaboration criteria.

2. Session Presentations

2.1 Session 1: Architectures, Protocols and Environments for TSD of future Polymorphic Networked ICT Systems

Co-Chairs: Neeraj Suri (Technische Universitaet Darmstadt, Germany) and Paul Barford (University of Wisconsin, US)

Rapporteur: Michael Bailey (University of Michigan, US)

Session Participants:

Marc Dacier, EURECOM, France	Ravi Iyer, University of Illinois, USA
Pieter Hartel, University of Twente, The Netherlands	George Kesidis, Penn State Univeristy, USA
Eric Luiijf, TNO Defence, Security and Safety, The Netherlands	David Kotz, ISTS—Dartmouth College, USA
Michel Riguidel, ENST, France	John McHugh, Dalhousie University, USA
Reijo Savola, VTT, Finland	Klara Nahrstedt, University of Illinois, USA
Neeraj Suri, TU Darmstadt, Germany	Vern Paxson, ICSI/LBNL, USA
Tom Anderson, University of Washington, USA	Wade Trappe, Rutgers University, USA
Michael Bailey, University of Michigan, USA	Takashi Nanya, University of Tokyo, Japan
Jody Westby, Global Cyber Risk LLC, USA	Jacques Bus, European Commission, EU
Paul Barford, University of Wisconsin, USA	Karl Levitt, NSF, USA
Carl Gunter, University of Illinois, USA	Helen Gill, NSF, USA

2.1.1 Session Preparation

Prior to the event, the participants of this session were asked to prepare the following set of questions:

1. "What do you foresee as the key challenges in specifying S&D in unstructured and unbounded future IT environments?"

   The question elicited a number of responses regarding the expected infrastructure characteristics of such an environment including:
   - Scale
   - Heterogeneity
   - Dynamics (including trust)
   - Mobility/accessibility
   - Pervasiveness
   - New technologies
   - Anonymity versus attribution
   - Diverse legal and policy frameworks
   - Diverse threats and vulnerabilities.

   There were also responses regarding new requirements for the environment including the need for:
   - Specification methods (nomenclature) and metrics
   - Continual re-specification.

The co-Chairs brought also for discussion the following additional issues:

- What are the requirements?
- Tussle between specifying details of the future environment and risk of missing the mark. What is the right target?
- Do old technologies hamper the creation of new technologies and how?
- How are threats and vulnerabilities included in the environment specification?
- Are there differences between EU and US specification objectives?

The following additional relevant aspects were also identified as issues to consider:

- Legacy vs. clean slate [approaches]
- Definitions of trust, security & dependability
- Framework: technical vs. legal vs. societal
- Trust and security metrics
- Interfaces between security mechanisms
- Touchstones for international collaboration.

2. "What do you foresee as the key technical issues in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?"

The responses received were referring again to the increasing complexity, diversity and scale, but were also providing a number of other issues in the characterization and scoping of the environments:

- Understanding where we are now so we don't make the same mistakes in the future
- Moving targets everywhere
- Building in monitoring capability
- Building in S&D capability (where and how)
- Defining/expressing trust properties and security policies
- Legal and regulatory frameworks (U.S. vs. EU)
- Understanding social and cultural issues
- Accommodating private/local S&D requirements
- Global environment and global threats.

The co-Chairs brought also for discussion the following additional issues:

- Tussle between emerging applications, services, technologies and S&D requirements
- Anonymity vs. attribution
- Priorities for building S&D into future architectures
- Theory vs. practice
- Models and mechanisms for trust.
- Constraints vs. innovation
- Data sharing vs. privacy
- Abstractions and mechanisms for secure architectures
- Specification vs. implementation.

3. "What sort of test beds, data sets, and models for evaluation and validation are required for assessing S&D architectures, protocols and system/service environments?"

The responses received pointed to the need for the establishment of test beds as potential mechanisms for future collaboration. Realistic and scalable test beds are needed for:

- Mobile devices
- Edge through core evaluation

- Interoperability
- Enabling the ability to faithfully recreate network conditions
- Enabling validation mechanisms.

It was also pointed out that there is a need to assess current test beds before creating new ones to prevent the inclusion of the problems they are designed to solve! There was also a request for development of models for attacks; a need for diverse, standardized empirical data sets taking into account the tussle between privacy and required detail; and, testing of ideas for future technology with available as-is technology.

Some of the discussion points/issues elicited from these responses included:

- What are the strengths/weaknesses and future role of emulation-based test-beds like DETER and PlanetLab?
- How can the $750M investment in GENI be maximized; in particular, can this be assisted with international cooperation?
- How can we increase the size, diversity, availability, utility of empirical data sets?
- Tussle between control/repeatability and realism.
- Is there something that we are missing?
- Understanding the limitations of test beds
- The need for in-situ testing
- Knowing and understanding the legal limits of data sharing.

2.1.2 Session Results

The participants of the session first discussed the focus of Theme 1. They agreed that this was centred on:

"Interconnections between diverse computing environments and networks is an evolving reality while security and dependability (S&D) to support trustworthy use is lagging. To address long term S&D issues in diverse and evolving networks, a clear characterization of this environment is required."

There were questions regarding the approaches and perspectives that the discussions should entail, whether concentrating on evolutionary technologies (Internet of 3-10 years out) versus disruptive technologies (clean slate designs). There were questions about the utility (or futility) in characterizing a moving target. There was a need to discuss the effect, even in clean state designs, of legacy networks, code and behaviours and whether it was simply a matter of composition and scaling of the properties of heterogeneous systems.

It was also stressed the need to include in the discussions requirements not only in the core technical environment. In particular, one should take into account a number of appropriate perspectives including legal, social and cultural as well as the roles and viewpoints of other stakeholders (operators, users, service providers, etc.)..

The definition of what is meant by and where "security" should reside were discussed: whether it was securing the devices and/or providing security services and whether it should reside at the client level or the network level or both. Techniques for enhancing security were discussed including the Trusted Platform Module in Trusted computing. The fact that availability and dependability of the networks can change for reasons other than security was discussed as were tradeoffs like privacy versus policy and expanding applications capability versus restricting them with security & dependability. It was felt by the participants that applications increasingly define the problems you want to solve in these environments.

The difficulty of setting up test beds in these new environments was highlighted due to the lack of knowledge about what needs testing. A number of potential approaches regarding test beds were discussed

including testing a single hypothesis or building a general facility for testing. The track record for general test beds, especially in the security and dependability environments, is poor. There is a distinct need for "real" environments for testing.

The session also focused on a number of research challenges that would benefit from mutual international collaboration within Theme 1. These included:

1. **Global Identity Management.** Focusing on the Identification of what is meant by identity i.e. program or code, virtual avatar, device, person, disaggregate views of oneself based on context (for example, use of different credit cards).
2. **Attack Attribution.** Defined as "Information concerning possible attacks, who or what is responsible for the attack, the extent of the attack". The tracking or tracing of attacks is critical to enable prosecution of cyber criminals. However, this must be adequately balanced with the technology challenges, legal policies and privacy of individuals.
3. **Interdependency of systems.** The objective of this research challenge is to understand the impact of a federation of heterogeneous ICT systems. A number of interdependencies were highlighted including ICT and power systems and ICT and financial networks. Conversely, within this research challenge, it would be necessary to consider the effect of previously unconnected networks; for example, the Internet and aircraft control systems.
4. **Test beds and datasets.**

   Test beds: There is first a need for well defined testing methodologies. A number of approaches to testing were discussed including: emulation, which enables repeatability testing and pre-testing of disruptive technologies; at-scale, real-world, field testing, which highlights the gap between expectations and reality and enables measurement and reactions. It was agreed that both of these approaches are necessary for test beds dealing with security and dependability because the gap is sizable whereby the attacker defender models are highly evolutionary, and the risk is substantial with worms released and proxies within attacks. Moreover, getting the emulation details correct is made difficult especially due to bot-nets and multi-stage infections.

   Datasets: Opportunities for international collaboration regarding datasets are quite large given the different global contexts e.g. social, cultural and legal and the different characterizations of parameters e.g. users, usability and mobility patterns. There are also cultural issues for how we provide datasets that would need to be addressed and there could be an approach of rewarding data set publication. There are also other issues with sharing data including a "diluted glory" factor and the methodology for the safe release of data. Another approach of actively promoting and attributing the contribution of datasets could be taken (e.g., bibtex dataset entry). In summary, international collaboration on approaches and techniques for measurement would be an enabling technique for test beds and datasets, but there are serious legal and policy considerations that must be addressed in the process.
5. **Policy and Interfaces.** The overall objective of this research challenge is to define the interfaces between heterogeneous systems. A determination must be made whether it is a legacy and/or clean slate network design required and take into account the evolutionary changes as the result of services/application-driven environments. The diverse policies of these networks, communities, and governments have variable parameters, which must be factored into the research from the start including technical and non-technical aspects (socio, legal and cultural), defining what is being protected from whom and identifying the likely threats.

2.1.3 Mechanisms for joint collaboration

There was a lengthy discussion regarding the establishment and need of a multidisciplinary security and dependability project to incorporate all of the relevant stakeholders needed to address the privacy and legal considerations for global cyber security. There are already a number of consumer expectations about privacy and organized policy centres, in both the US: e.g., Electronic Privacy Information Center (EPIC)and the American Civil Liberties Union (ACLU); and in the EU: e.g., Statewatch, monitoring the state and civil liberties of Europe, EDRI, monitoring the Digital Civil Rights in Europe and the European Civil Liberties Network, launched in October 2005 as a long-term project to develop a platform for groups working on civil liberties issues across Europe. These policy centres viewpoints should be incorporated into the research work of the S&D communities.

A number of legal considerations in cyber security that need to be considered include:

- Test data sets of traffic data may contain packet headers comprised of IP addresses and port information as well as packet content consisting of personally identifiable information (PII), content, and URLs.
- Privacy laws and regulations around the globe pertain to PII, IP addresses, and protected types of information, such as financial, health, and employment data. The privacy laws and regulations around the globe are inconsistent, causing significant cross-border data problems and complicating cyber security R&D. For example, within the U.S. there are federal laws and a patchwork of privacy laws in 50 states. The EU legal framework governs 27 member countries. More than 20 other countries are also enacting laws and regulations regarding privacy and security of data. Cross-border data flows between the US and EU are hampered by requirements for consent to send that data out of the EU or another form of cross-border "permission" in the form of contract clauses, the use of Binding Corporate Rules, or participation in the US Safe Harbour program.
- Other legal considerations are associated with federal regulatory actions that have interpreted privacy policies as implied contracts and the public's expectations of privacy. Information sharing that is critical to tracking and tracing is also problematic. Issues arise concerning opt-in or consent requirements to share information, confusion regarding who is the owner of data and mutual recognition of clearances.
- Significant legal issues arise regarding access by "governmental entities" (including government researchers) to traffic data. This is tightly controlled by the Electronic Communications Privacy Act, which governs wiretaps and access to stored electronic communication data.

The establishment of a Deterrence Framework to counter cyber-crime should include the following:

- Cyber-crime laws (crime, circumstances damage, penalty);
- International cooperation (multilateral assistance treaties, letters rogatory, dual criminality, extradition);
- Rules of criminal procedures (search and seizure, evidentiary).

The conclusion was that there should be established a multidisciplinary co-operation project driven by a core EU/US working group (as shown in Figure 3). Its main aim would be to bring together the International R&D community in the field of security and dependability with other identified non-technical stakeholders that would have a vested interest. The purpose of the project would be to create a collaborative environment where multiple cyber security considerations can be taken into account in a holistic manner to avoid stove-piped solutions. Collaborative efforts are essential to solving today's cyber threats and to finding ways to channel R&D to accommodate the myriad of issues that impact present and future research programmes in ICT for Trust, Security and Dependability.

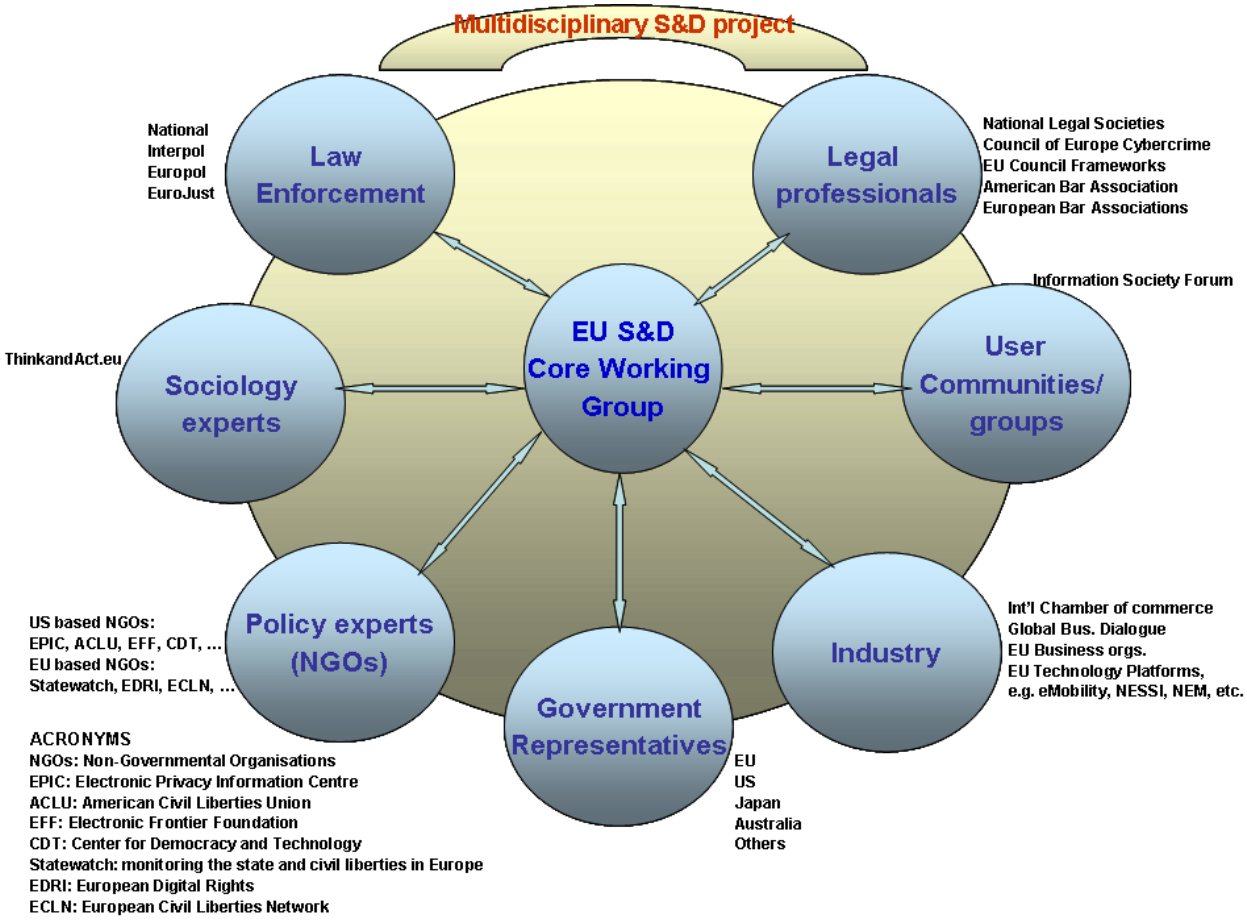


Figure 3: Multidisciplinary Security & Dependability international cooperation project

The central areas that are common to all participants in countering cyber security issues are:

- Blocking and preventing malicious acts or code
- Tracking and tracing
- International cooperation
- Information sharing

Without progress in these basic areas, cyber-criminals will continue to win. Cyber security R&D is desperately needed to address basic issues in each of these areas because problems in these areas thwart efforts to counter cyber criminal activities. Related subtopics include:

- Forensics
- Metrics
- Information system self-healing
- Laws and regulations
- Mutual recognition of clearances or approvals for information sharing.

2.2 Session 2: TSD Attributes and Mechanisms for future Distributed Services and Content, future Overlay Networks and Applications

Co-Chairs: David Nicol (University of Illinois, USA) and Roberto Baldoni (Università di Roma "La Sapienza", Italy)
Rapporteur: James Clarke (Waterford Institute of Technology, Ireland)

Session Participants:

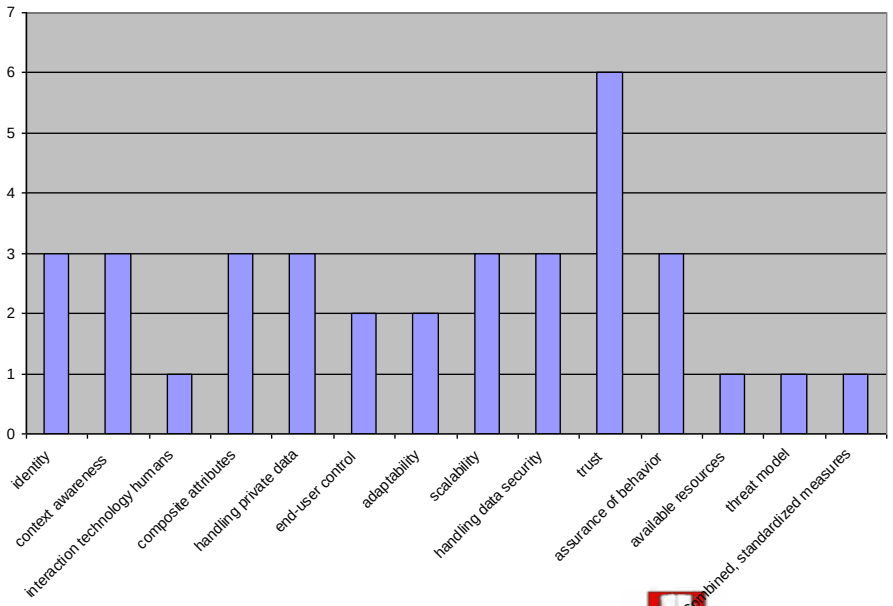
Roberto Baldoni, Università di Roma "La Sapienza", Italy	Richard Kemmerer, UC Santa Barbara, USA
Robin Bloomfield, City University London, UK	Roy Maxion, Carnegie Mellon University, USA
Sandro Bologna, ENEA, Italy	David Nicol, University of Illinois, USA
James Clarke, Waterford Institute of Technology, Ireland	Michael Reiter, Carnegie Mellon University, USA
Fabio Martinelli, National Research Council, Italy	William Sanders, University of Illinois, USA
András Pataricza, Budapest University , Hungary	O. Sami Saydjari, Cyber Defense Agency, LLC, USA
Aad Van Morsel, University of Newcastle, UK	Alfonso Valdes, SRI International, USA
Nikita Borisov, University of Illinois, USA	Jason Smith, Queensland University, Australia
Elsa Gunter, University of Illinois, USA	Douglas Maughan, Department of Homeland Security, USA

2.2.1 Session Preparation

Prior to the event, the participants of this session were asked to prepare the following set of questions:

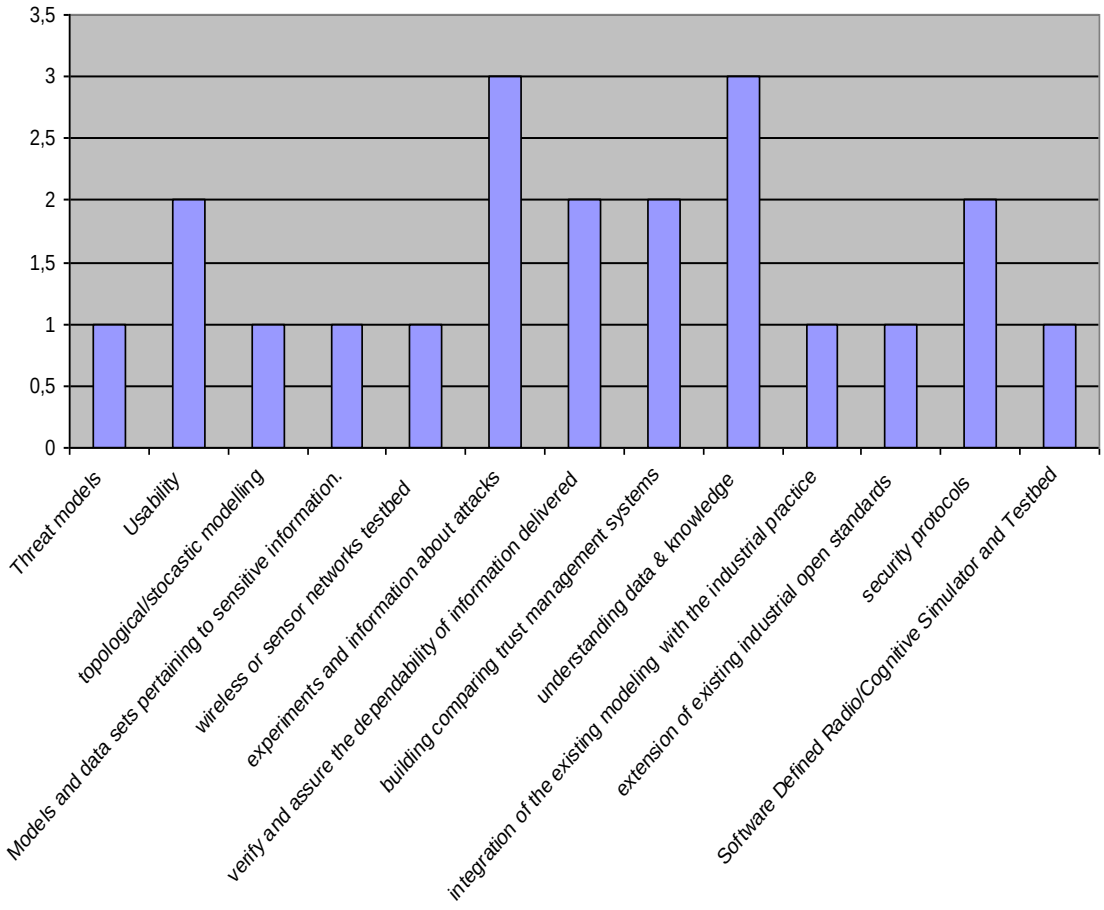
1. "What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?"

   The responses received are reflected in the Figure below:



2. What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

   The responses received are as follows:



3. What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

   Again, the responses received are as follows:

2.2.2 Session Results

The participants of the session focussed first their discussions in getting a common understanding of the terminology that was being used in the theme description. For example, the word "polymorphic" was discussed and consensus on its meaning was *describing a large system characterised by many stages, and with dynamicity and heterogeneity of connection(s) of systems*. Other characteristics of a polymorphic multi-mode environment (MME) include: the abstraction of service will be prominent, flat layering between communication and software services will be less and less clear, peer-to-peer (network and software services) can be added/removed at any time, scalability, dynamicity and legal issues will be extremely important.

The fundamental difference between Theme 1 and Theme 2 was also discussed. It was agreed to look at these themes like a layered approach: Theme 1 is addressing the system architectures, protocols and environments for S&D of future systems, whereas Theme 2 is addressing the attributes and mechanisms required to provide and enhance the S&D for the system architectures, protocols, environments. It was also felt that models as such are part of theme 1 but that theme 2 is addressing the attributes (requirements and specifications, etc.) **needed to define** the appropriate models (trust, security, resilience, etc.).

Once the terminology was agreed, the session participants began discussions following the template presented in the plenary session. The template consisted of the following items:

a. What research challenges and, maybe, applications should be a priority? (give specific examples)
b. Why should they be a priority?
   - Technical reasons progress can be made
   - Urgency to address
   - Why international collaboration is critical
c. What are the mechanisms for collaboration that should be employed and why?
d. How can advanced test beds, models, and datasets facilitate the research?

The discussion permitted to identify a number of R&D challenges for International collaboration.

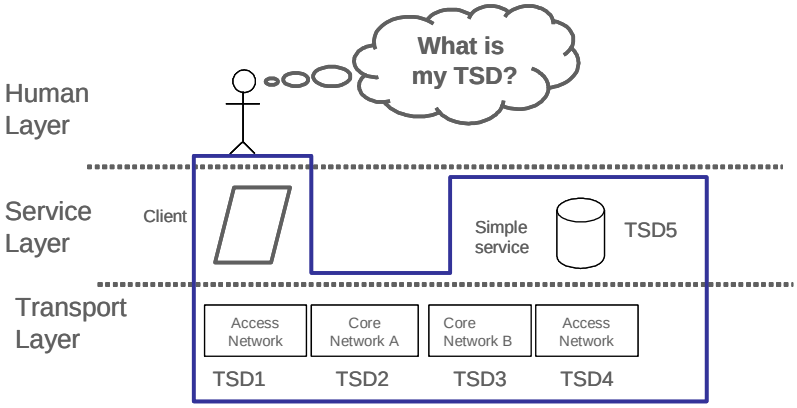
1. **Dynamic service coalitions → Dynamic service virtualisation in polymorphic (MME) environment.**

   1a. what research challenges and, maybe, applications should be a priority? (give specific examples)

   The overall goal of this research challenge is controlling the delivery of atomic or complex services to end user (human or other service(s)). A verifiable and enforceable contract needs to be behind with some guarantee that will make services more trustworthy and comfortable for the user to use them. This challenge has the elements of dynamicity, trust with respect to services and negotiated contracts establishment over unknown global paths in real time. Services, which have to be trustworthy and held accountable, must traverse several components of the networks, which could be located anywhere in the world with different legal aspects that must be taken into account. The IT infrastructure nowadays is getting more and more distributed. For example, eBay is pioneering in this as they are doing business in different places. The approach to be followed should be to use the existing Service Oriented Architecture (SOA) and enhance it to make the next generation internet more trustworthy, secure and dependable.

   The participants discussed a scenario in which a software service could be composed by an orchestration of other services.

   The figure 7 below contains a depiction of a simple software service delivered to an end user through an MME.



Important Notion: Information Channel

Figure 7: Simple software service in an MME

Figure 8 shows the explosion of complexity in an MME when the number of potential services that could be orchestrated as required by the user services are multiplied.

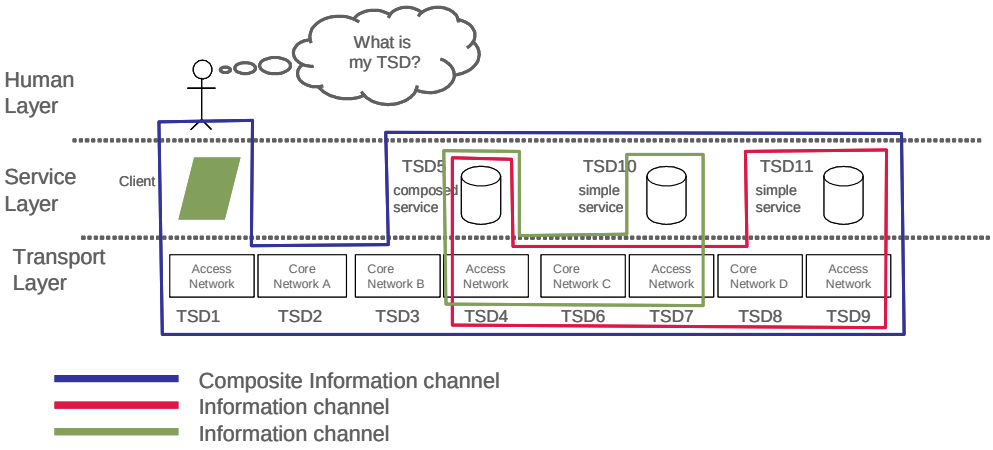


Figure 8: Complex software service in an MME

1b. Why should they be a priority?

Technical reasons progress can be made: Technically, we must understand the policies in all the different environments to correctly design and build the systems to provide the necessary trust, security and dependability for the next generation Internet. People sometimes go for the telephone because they are secure in the knowledge that no one would hear them. When you talk about the future Internet, you need to provide a similar scenario with a trusted service that can be reached safely to invoke this comfort level with the user. We need to be able to instil users' faith in services. We need to enable services to be properly certified. There is currently a lack of methods because we don't know exactly how to measure Trust. A credible way of doing this would be to collaborate on an international scale on the metrics required to measure the level of security and dependability properties.

Urgency to address: These things are starting to happen now on a global basis e.g. eBay, etc. If you have a good architecture for SOA (secure, dependable, etc.), there would be much more impact gained and higher take-up. In order to be successful, we must harmonize the efforts within the Security & Dependability communities and the Software and Services communities. If you do not do it now, it will be too late. This will also enable B2B for supply chain and critical infrastructures, which will be a significant benefit to all concerned.

Why international collaboration is critical: A number of reasons were identified here. There are specific rules, laws, and cultural aspects for trust and privacy in different countries that must be researched in a collaborative fashion. The high degree of heterogeneity required for dynamic service coalitions needs the awareness of everyone involved so you have an underlying basis for interoperability. There are different policies over the boundaries crossed in this environment. The services will have to match policy on the fly, which, in turn, needs global co-operation. It is not efficient in the development phase to make assumptions about what the other countries policies are, as there will almost certainly be incorrect assumptions made, which will require a re-development phase. It was also pointed out that the challenge fits well the "complementarity" criteria, because the US researchers are not spending that much research time on this subject whereas the EU researchers are. Therefore, there would be significant synergy for them to work together to save on overlapping research time and efforts. There are also a significant number of different cultural and legal aspects that must be addressed in this challenge. Participants stressed that some of this work needs a certain critical mass with international collaboration in order to leverage momentum and achieve more credibility and impact within the standardisation community.

1c. What are the mechanisms for collaboration that should be employed and why?

See section 2.2.3 below.

1d. How can advanced test beds, models, and datasets facilitate the research?

See item number 4 below.

2. Targeting specific applications for TSD, e.g., finance, e-health

2a. What research challenges and, maybe, applications should be a priority? (give specific examples):

The overall goal of this challenge was identifying deployment environments for developing and testing TSD critical applications, for example, financial and e-health. There are cross-border privacy elements resonating in many contexts with both of these applications. A number of other applications were also identified including critical infrastructure (e.g. power oil, gas, water) applications that are increasingly using SoA, attempting to build trustworthy systems with untrustworthy components.

2b. Why should they be a priority?

Technical reasons progress can be made: The strength of formal methods on the EU side can be brought to bear to help the GENI test bed, which could then be further extended to other places around the world.

Urgency to address: it is critical to address this challenge in order to identify the needs and requirements related to strengthening the S&D of these kinds of applications.

Why international collaboration is critical: The financial industry has international regulations so there is a strong need to work together to get these factored in. e-health bears a similar situation whereby in the future, it is conceivable that you solicit a doctor who is located somewhere else in the world and not locally to read your x-Rays. It was also deemed highly appropriate with these global applications to gain access to crucial domain knowledge / expertise in another nation if there were identified strengths found to address key problems in a mutually beneficial way.

2c. What are the mechanism for collaboration that should be employed and why?

See section 2.2.3 below.

2d. How can advanced testbeds, models, and datasets facilitate the research?

See item number 4 below.

3. Establishment of Data-Sets handling rules and guidelines.

3a. What research challenges and, maybe, applications should be a priority? (give specific examples)

The overall aim of this challenge is keeping up-to-date, detailed documentation of the data sets, which is considered an important research challenge.

3b. Why should they be a priority?

Technical reasons progress can be made: If the data isn't accompanied by an appropriate level of documentation, it is useless or it can be wrong and/or misleading if not explained properly. There needs to be a standardised way of keeping the data in a repository so that the data is in the same format every time. Results are then more believable, relevant, reliable and useful.

Urgency to address: The Urgency to address is critical as datasets cannot be used reliably without it.

Why international collaboration is critical: In order to exploit and make use of a data warehousing approach to analyze, cross-exploit and share test bed results enabling knowledge collection and management, there would have to be agreement on datasets repository and document formats from the international communities involved.

3c. What are the mechanism for collaboration that should be employed and why?

See section 2.2.3 below.

3d. How can advanced testbeds, models, and datasets facilitate the research?

See item number 4 below.

4. Establishment of mutually beneficial Joint Test beds

4a. What research challenges and, maybe, applications should be a priority? (give specific examples)
A number of joint test beds were discussed. These included:

- Software and Services
- Federated wireless and wired networks
- Intermediate level test beds e.g. cross jurisdictional policy issues, financial or medical records databases.

4b. Why should they be a priority?

Technical reasons progress can be made: Significant progress can be made with the establishment of a large international project with many complimentary groups.

Urgency to address: The financial and e-health systems will need the global aspect as previously discussed. Collaboration is needed in order to develop a ***methodology for international experiments.***

Why international collaboration is critical: We should build upon the strong points of each country: For example, the US is strong on the lower networks level and the EU is strong on the service and application levels and formal methods (for example, this could be used for on line access control in platforms like GENI. We must build on this synergy).

Targeting specific applications e.g. financial, e-health deployment environments need to be first defined for testing such an application (related very much to challenge 2 above). Putting requirements in place on an international basis would be difficult due to the differing laws, rules and regulations involved. However, it wouldn't be impossible and there is a need to work together to get these international regulations factored in.

A number of additional research challenges were identified in the brainstorming part of the session, which, due to time constraints, were not dissected in as much detail as those described above. These challenges need to be addressed in more detail at a later stage:

- **Privacy coalitions.** In the US, individual States have different privacy laws. US researchers are trying to look at metrics for risk exposure by taking all the States laws and measuring/analysing whether the data is risky. Some of the US participants proposed, therefore, that when trying to understand privacy in the US, it would be useful to look at how the other countries handle it. The EU has made technical progress in this area; for example, emphasis on purpose and obligation are already in the EU laws.
- **International Law enforcement over the Internet.** A radically different approach needs to be taken given the increased instances of spam and exploitation over the Internet. There has to be established an international Internet governance covering these areas. For example, at present, laws can be passed in the originating country but are potentially un-enforceable where the actual damage occurs.
- **Software assurances.** There are numerous significant developments in advancing programming languages and tools for improving software quality, but much more needs to be done. It would be very worthwhile and more efficient to carry this out on an international scale.
- **The need to focus on all aspects of ICT.** There is a need to address also the telecommunications systems dependability and to not focus on the Internet only. A global multi-disciplinary approach should be taken and lessons could be learned from each other on how these elements are addressed and to determine how faults of these polymorphic systems would impact the everyday users of all ICT elements.

2.2.3 Mechanisms for Joint collaboration

Mechanisms were discussed that could potentially be used for moving forward the identified research challenges for mutual collaboration. These included:

- Setting up large scale projects addressing specific problems to produce medium term outcomes (5 years) that would involve 10-20 groups with the required skills for transatlantic cooperation.
- Other smaller co-ordination type mechanisms that would be needed to facilitate, drive and set up this kind of an activity within the current financial mechanisms that are available from the funding organisations. A number of already existing working models were discussed and were thought might provide some insight into how it could be applied to the International Security and dependability community. One example is within the Physics domain, e.g. CERN. A question was raised whether it would be feasible to set up an International Dependability centre modelled around the CERN model.

The need to make the research calls and evaluations synchronised with each other was stressed, for the system to work properly. Regarding the use of datasets, joint projects would need authoritative (granting program management) support to gain access to data to make the research a real possibility.

Other possible cooperation mechanisms discussed included:

- Establish a joint programme in which the content is evaluated thoroughly by one side technically and, if accepted, each side evaluates the financial elements individually and pays their members separately yet in a coordinated fashion. This is similar to the mechanisms the EU programme previously used for

Associated Member States (EA) e.g. Switzerland, when they were allowed to be full participants to the European Commission projects while still being funded by the Swiss government.

- In each project proposal, have fraction of funding reserved for international collaboration to be drawn down on an as needed and evaluated case by case basis.

3. Final Conclusions

The outcomes of the two successful workshops held on "Cyber Trust: System Dependability and Security" make it clear that key decision makers at programme level in the European Commission, the United States National Science Foundation and Department of Homeland Security, the Japan Science and Technology Agency and the National ICT Australia programme and key researchers from the EU, USA, Australia and Japan are committed to engage in the process of establishing co-operation frameworks in the discussed areas of research.

The **outcomes** of this workshop included the following:

- Convergence on technical themes to address: what are they, why now and how to validate;
- Convergence on collaborative research topics;
- Discussion of realistic mechanisms and approaches for international cooperation;
- Start to plan potential project areas for international collaboration;
- Start laying the groundwork and path of future International collaboration activities.

Within the intensive working group sessions of the workshop, a number of research topics were considered as beneficial and necessary for continued mutual collaboration on an international scale.

Theme 1: Architectures, Protocols and Environments for TSD of future Polymorphic Networked ICT Systems

- Global Identity management – coming to a consensus on the classification and meaning of identity: Program or code, virtual avatar, devices, persons, different views based on context;
- Attack distribution – "information concerning possible attacks, who or what is responsible for the attack, the extent of the attack"[2] , information gathering; tracking and tracing for forensics to enable prosecution of cyber criminals; balancing technological challenges with legal aspects and privacy of individuals;
- Interdependency of systems – need to understand the impact of federation of heterogeneous ICT systems (for example, ICT and control systems and ICT and financial networks); may wish to consider the effects of connecting previously unconnected networks (for example, the Internet and control and communications systems). An example used to illustrate this potential challenge and complexities was the Internet and aircraft command, control and communications systems;
- Test beds and data sets – need well defined testing methodologies and approaches to testing (for example, emulation, at-scale and real world); both test beds and datasets for Security & Dependability need to cater for large gaps and risks; need to address difficulty of obtaining data, as well as some specific issues surrounding the sharing of datasets (for example, "diluted glory" and how to safely release the data; measurements as an enabling technique for test beds and datasets);
- Policy and interfaces – need to define the interfaces between heterogeneous systems: are they legacy/clean slate network designs or (r)evolutionary changes as the result of having to adapt application driven environments. Autonomic, evolvable and adaptive security policies and mechanisms and new cognitive techniques and semantic models for managing the complexity and interdependencies of ambient systems and their interaction with users are needed.

[2] Taken from Infosec Research Council Hard Problems List - see http://www.**infosec**-research.org/docs_public/IRC-**HPL**-as-released-990921.doc

Theme 2: TSD Attributes and Mechanisms for future Distributed Services and Content, future Overlay Networks and Applications.

- Dynamic service coalitions, dynamic service virtualisation in polymorphic (MME) environments. Composition of trust; Service Oriented Architectures; Scenarios for composed services.
- Privacy coalitions (risk metrics);
- Targeting real world applications (finance, e-health, including cross-border privacy; Critical Infrastructure Protection). Building trustworthy systems with untrustworthy components.
- Exploitation of complementarity in respective technical strength areas; For example, U.S. research is more concentrated on lower network levels whereas EU research concentration is more on the middle and higher applications and services layers;
- Mechanisms to create large continuous projects; joint EU-US proposals; synchronisation of calls;
- International Collaboration: critical mass is needed but at the same time multicultural/legal environments need to be maintained and will create the added leverage leading to standardisation;
- Data-sets: protection and repository methodologies including documentation need to be developed to provide useful and long term efficiency with use of data-sets;
- Joint test beds: Software and Services; Federated wireless and wired networks; intermediate level (cross jurisdictional, e.g. in e-health and financial sectors);
- Software assurance cases, metrics & measurement, and assessment in general.

The expected outcome of starting to plan potential international project areas came to fruition also as a number of potential project ideas that were discussed by the participants during the workshop. Particularly interesting subjects for multidisciplinary S&D projects at an international level were:

- A Co-ordination type project that would act as catalyst to facilitate, drive and set up future activities in a systematic fashion to enable and assist the continued international collaboration;
- Privacy and legal considerations for global cyber security involving all relevant stakeholders (researchers, technologists, government, policy, sociology, consumers, etc.);
- Dynamic service coalitions in polymorphic diverse computing and network environments controlling the delivery of atomic or complex services to end users with a verifiable and enforceable contract behind that could provide some guarantee for the delivery of more trustworthy and comfortable services to the user.
- International Test beds, establishment of, and/or connection of existing standalone test beds and validation and sharing of datasets at an International level.

Throughout the workshop, a number of realistic cooperation mechanisms were presented by the European Commission, the National Science Foundation and the Department of Homeland security that were based upon existing research programmes. These could benefit researchers directly and help build up stronger international collaboration in the future. The Japan Science and Technology Agency and Australia's NICTA have indicated willingness to run a parallel programme that could work alongside the EU and US efforts to help funding international research in Trust, Security and Dependability. .

Appendix A – The Organising and Steering Committee Members of the Illinois workshop

Molly Tracy, University of Illinois, USA

William Sanders, University of Illinois, USA

Farnam Jahanian, University of Michigan, USA

Jim Clarke, Waterford Institute of Technology, Ireland

Brian Randell, Newcastle University, UK

Michel Riguidel, ENST, France,

Karl Levitt, NSF, USA

Helen Gill, NSF, USA

Douglas Maughan, DHS, USA

Jacques Bus, European Commission, EU

Thomas Skordas, European Commission, EU

Appendix B – Participants Pre-Workshop Inputs to Sessions

Theme 1: Architectures, Protocols, and Environments for S&D of future Polymorphic Networked ICT Systems

Michael Bailey, University of Michigan

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

(i) *Heterogeneity and scale.* The next generation of networks will be composed of hundreds of thousands of unique devices and application types and trillions of networked devices. While the problem of scaling S&D solutions to this level is daunting in and of itself it is perhaps the heterogeneity of these systems and applications that is the biggest threat to future security. Each new device and application brings with it its own proprietary code base and opportunity for exploitation.

(ii) *Mobility.* As connectivity becomes increasingly pervasive and devices and technologies more and more converged, users are becoming increasingly mobile. Addressing this mobility creates not only problems in standard connectivity such as addressing, routing, capability discovery, etc., but also in securing existing systems. As users move in and out of historically secured environments (i.e., wall gardens) they expose the enterprises and organizations to which they belong to increasing risk.

(iii) *Increased pervasiveness and invasiveness.* While pervasive connectivity and the emergence of home networks and the use of sensor and actuator networks have offered users a new level of control over their devices and environments, the potential risks of these systems are troubling. Information previously only available through human reconnaissance (e.g., are you on vacation?) is now increasingly easy for savvy attackers to access and utilize. As a result, we run the risk of encouraging a trend away from risk against our virtual selves (e.g., credit identity) to our physical selves and property.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

(i) *Lack of consensus on key design issues.* One of the most limiting factors in our ability to effectively understand and address the impact of these challenges is our fundamental lack of consensus on the key design issues for the next generation networks. Should security be built into the infrastructure (e.g. built into routing infrastructure) or should control plane be moved out of the router, offered as a secure robust service? If a service, where should the protection take place: in the network cloud or at the edge (e.g., the end-to-end dilemma)? Does (router and network) virtualization solve or exacerbate infrastructure security problems?

(ii) *Lack of indicators for understanding scope.* The new technologies, architectures, and deployments of future ICT systems will result in a fundamental shift in the way users utilize computing resources. Currently we can only speculate on such key items such as the scale of these systems, the degree of heterogeneity of devices and applications, adoption rates, etc. In addition, we have even less confidence in our ability to predict how the users of these new capabilities will use these systems and will interact with their environments and other users.

(iii) *Existing trends in security.* Recently, threats have undergone a dramatic transformation, away from attacks on availability, to attacks on privacy. This evolution of malicious Internet activities

primarily motivated by economic incentives and includes activities such as DoS Extortion, Identity Theft, Phishing, SPAM, and Spyware. In order to perform these types of attacks, malicious users need an anomalous delivery platform for launching their attacks. Rather than vandalize existing network hosts or take them off the network, the attackers now use them to make money. Understanding the threat models and their evolution is key to charactering the solutions for S&D in ICT systems.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

(i) *New Models for mobility and interconnectedness.* One of the key problems in defining the scope of these new systems is understanding how the users of these systems will interact with their environment and each other. Preliminary work in mobile computer environments such as Bluetooth or automotive networks have suggested that the connectivity properties of these systems are very different from traditional mobile users (e.g., laptops). To be effective, we need models, datasets, and tools that help to characterize these new behaviour patterns.

(ii) *Edge and core testbeds.* Enterprise networks hold the vast majority of hosts in the network and are the key drivers of new applications and services for the network as a whole (e.g., messaging, VoIP). The different goals and properties of enterprise and backbone networks (e.g., host verses router, fixed verses mobile, open verses closed) necessitate testbeds that account for these differences. The creation of new enterprise testbeds, or the expansion of existing testbeds to better account for the unique properties of enterprises, offer an excellent opportunity to explore S&D issues associated with new ICT networks.

(iii) *Real world testbeds and datasets.* New ICT systems will require new protocols, applications, etc. These new ideas will be hard to validate because they will be based on functionality that may not exist and may be disruptive to production networks. In order to address the important limitations of existing approaches such as modeling or simulation we will require large scale production like testbeds that are capable of executing as many of the various new properties of next generation ICT as possible (e.g., mobility, pervasiveness, heterogeneity). These testbeds will need to be driven by realistic workloads: either those of actual users, or those derived directly from them.

Sandro Bologna, ENEA

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

Most challenging will be the capability to consider all together all the different elements of future unstructured and unbounded ICT environments, like:

- Software (errors in coding, patches, …)
- Hardware (components faults, …)
- Payload (mis-authentication, encapsulation of malicious content, …)
- Network (interconnection, interoperability, points of concentration, …)
- Environment (dependence on external elements, electromagnetic effects….)
- Human (forgetfulness, distractibility, …)
- Organizational (job function, corporate culture, …)

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

The test bed should support interoperability testing. Testing of these interactions is a complex process. Interoperability testing should be supported by procedures and an agreed set of tests that should be

executed prior to the connection of an ICT environment (network) to already existing one. Feature interoperability can be provided by either feature emulation or simulation. Standardized interoperability testing procedure and test data sets should be agreed.

Nikita Borisov, University of Illinois

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

Traditional Internet infrastructure provided few guarantees, pushing most security and dependability concerns to the endpoints.

In the future, networked infrastructure may be tasked with providing QoS and other guarantees, as well as providing security services such as supporting authentication, audit, and privacy protection. Further, there is an emerging computing infrastructure alongside the traditional network infrastructure that will become an increasingly essential part of applications and services.

The definitions of security & dependability for these new infrastructures will be different than the traditional definitions, since they must address issues of global scale, pervasive sharing across different, mutually distrusting administrative domains, and conforming with disparate legislation that spans national boundaries.

The scope and the scale of the problem naturally invites multi-national collaboration. The oft-conflicting requirements of security and privacy will need to be articulated with a good understanding of cultural norms and legislative protections across the world.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

A key architectural challenge is support for global monitoring of and coordinated response to attacks and other problems. Even now attackers routinely traverse organizational and international boundaries in order to make detection and response more difficult, and today's distributed attacks and worms are of such a scale that response at an individual or organizational scale is powerless to stop them. The trends suggest that these problems will be larger in magnitude in the future, and in addition, multi-modal attacks that exploit different types of infrastructures are likely to emerge. (We are already seeing attacks that exploit both cellular networks and the Internet.)

The need for global monitoring must be balanced with the privacy interests of organizations and individuals. Similarly, global coordination of responses must be balanced with the requirements for organizational and national autonomy, both to protect diverse interests and to avoid introducing new vulnerabilities whereby a response mechanism can result in global failures.

Once again, this problem is global in scale and involves an understanding of legal and cultural issues across the world.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

The models and test beds for simulation and evaluation of network architectures need to evolve from existing approaches, such as ns-2, SSFnet, PlanetLab and EmuLab. The extensions that will be needed should address the multi-modal, heterogeneous infrastructures, and issues of scale of the solutions. Further, as computing infrastructure becomes a larger part of the infrastructure, better support for it in the modeling and emulation frameworks will be needed.

The creation and distribution of data sets such as global network characteristics is currently done ad-hoc; a coordinated effort among international participants to collect such data and make it available to researchers is needed. Wider distribution of security-relevant data is also needed, and legislative barriers to sharing across countries must be overcome.

James Clarke, Waterford Institute of Technology

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

(i.) There are a number of Socio-technical challenges that needs to be addressed. Given that we are moving into an ubiquitous, mobile Information Society, with MME and continually evolving networked environments, the context for defining a new security paradigm in this new emerging Information Society is made very complex. The new security paradigm is distinguished by striking a reasonable balance between a Big Brother Society to a fully confident building and privacy and ethics protecting society (the Empowering the Stakeholder view as discussed at WS 1). The establishment of society's confidence in this new digital world requires the creation of a palpable defensive environment enabling citizens' control over the type and level of protection associated with the goods and services accessed or delivered through digital media. However, it must be clearly recognised that the means of providing this confidence should lie within an overall context of the citizens being able to live a free, unencumbered, comfortable and prosperous life: being protected against the risks of digital intrusion, crime, terrorism, etc., must not be seen as more of a burden than the risks themselves. In order to achieve this, ICT trust, security and dependability will need to become a matter of routine, and not be a source of potential problems and nuisance as often perceived today. Security and dependability will need to be a transparent, unobtrusive part of the operation of economic and social activity in a digital environment. To achieve this transparency, there needs to be a common taxonomy and terminology that is understood by all stakeholders. This will allow the development of a generalized, layered abstract model of security and dependability requirements and solutions that avoids the need for the users to know the detailed 'plumbing' of the underlying technologies.

(ii.) Federated identity management across these environments.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

(i.) There is a new world of the Internet, where boundaries are no longer clear and anyone can set up a network. To begin to deal with this situation, we need to build intelligence into networks so that rogue/malicious elements can be recognized and eliminated. Citizens must have this new Internet at their disposal with guarantees of privacy and confidentiality.

(ii.) There must be built in Monitoring for these systems to enable identification, study, prediction and prevention of re-occurrence of events. This should also encourage an approach whereby all stakeholders are involved in the examination of why or how a given system failure has happened. Specifically, there need to be approaches that:

- allow the determination of the extent to which the fault was human, some aspect of the system, or a component;
- enable a significant reduction in the probability that similar incidents will occur again;
- allow cross disciplinary investigation of incidents, including sociologists and other related disciplines;
- involve setting up a moderated global forum including all communities for sharing information of all aspects of network dependability and security.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

There were a number of test bed ideas raised and discussed at WS number 1 that I would like to see moved forward. An example of potential collaboration stems from the fact that the US side seems to have more facilities concentrating on the lower level (network) whereas in the EU, there is more concentration on the higher levels (services, applications). Therefore, the communities should leverage this synergy, for example, by establishing an application and software services test bed that could be built on top of GENI with a number of application level experiments. Planetlab runs a production level services platform and University of Berkeley is also building an experiments cluster, which may also be used for this purpose. It was recognised that there would be a significant amount of collaboration required as the middle layers, which provides the OS would need to be jointly addressed also. The underlying rationale for the establishment of this test bed was that the current experimental facilities, although open for unlimited experimentation, the focus is on network innovation. Therefore, it is left to the one's who want to run the experiment to set up from scratch the application, software and service environment. For SOA, this is not feasible for most especially SMEs and Academics. Therefore, if there was a software and services test bed 'playground' already set up, this would open up tremendous opportunities for others including innovative SMEs and academics to venture into service-oriented solutions, without having to endure the expense and complexities of setting up a full scale test bed.

Another test bed discussed was one for wireless or sensor networks. There are some standalone test beds already available but the issue that must be explored is to how to federate them taking into account cross testing, mobility aspects and security policy's as user's move in and out of different environments.

Regarding the mutual necessity and benefits of global co-operation that would justify and motivate the practicalities in establishing the co-operations with these particular answers, I believe they fit the categories because of the synergy expressed above for future testbeds and also for the socio elements raised, it will be necessary to work on these together in a global way in order to get it right the first time. We are also aware that the US side is also looking at the interdisciplinary approach similar to the EU side as expressed above in the socio elements answer to question a (reference: Institute for Security Technology Studies (ISTS) at Dartmouth College Newsletter Winter 2007) so this is an area we can work together.

Marc Dacier, Institut Eurecom

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

In such environments, S&D can not be expressed, specified, in classical static terms anymore. Moving away from classical Boolean visions, secure vs. non secure, we will have to investigate ways to specify S&D in fuzzier terms, may be probabilistic ones. This is not new for dependability but this will represent a challenge for security as this implies the quantification of security, the definition of metrics, the availability of sound fault assumption models, etc.

In these future ICT environments, S&D may have been to be defined not in absolute terms anymore but, instead, relatively to other attributes. As a result, S&D specifications may have to be defined as trade-offs between several conflicting objectives. For instance, strong authentication techniques may be CPU intensive, some reliable protocols may be expensive in terms of communication whereas small devices participating to pervasive, ad-hoc networks may not be ready (or able) to spend a large amount of their resources to help others.

Changing environments require S&D to be specified not only in terms of expected properties, verified -somehow- at a given point, but to be continuously assessed during the lifetime of the system under consideration. As a result, S&D specifications will need to include the specifications of methods for continuous online assessment of the expected properties. They will also have to include the definitions of "fall back" modes in case the observed security is apparently decreasing.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

These new environments will, most likely, be highly hybrid, reusing some of the existing infrastructures, taking advantage of new ones or even creating virtual infrastructures on top of classical ones (eg overlay networks). To cope with such complex and diverse environment, abstractions and layering mechanisms are typically used. For S&D to be meaningful, there must be a way to express and validate the expected properties of the underlying layers used. From a purely technical point of view, this is not easy. It gets even worse when we think that S&D properties may be threatened by the end user of the system itself, who is likely to make mistakes or to respond favourably to malicious requests (e.g. phishing attack, Trojan horses, etc..). Providing a convincing argument that all assumptions made to build an architecture that fulfils some S&D properties hold is a real challenge.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

In order to validate systems, their input domain space must be known. If it includes malicious inputs, they must be characterized as well. We will thus, therefore need representative data sets of malicious behaviours. A global initiative should be carried out to take advantage of the various specific initiatives that are taken in various places to collect such data (for instance using dark-nets, Internet telescopes, honeypots, etc.). Precise and scientific methods should be develop to assess the quality of these data sets, their complementarity. Techniques should be developed to overcome existing privacy issues that restrict the sharing of such data.

Carl Gunter, University of Illinois

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

One will be the management of keys and identities by naïve users. This as an ongoing problem for decades with the Internet and the problem gets worse as the number and usages of mobiles proliferates. One hopes for good solutions that work between administrative domains and transfer well as users move from one device to another.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

For security policies a central problem is the ability of users to understand policies they write or are faced with. There are major problems with current implementations so that only very rudimentary capabilities are available in practice. For example, delegation is still very difficult in many systems.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

For academic research a major problem is proving that techniques scale without having access to meaningful at-scale data. The nature of the type of access needed varies across domains, but a

common theme is lack of motivation by parties that own the data sets and potential concerns with confidentiality of personal or corporate data.

Elsa Gunter, University of Illinois

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

(i.) Being able to specify security policies in a manner that is at the same time expressive enough to handle diverse conditions (possibly based on the user's current needs and privileges, the trustworthiness of the mode of interaction, the authority and privileges granted them through various sources, to name a few)

(ii.) Being able to specify what knowledge can be extracted from a given authorizing (or identifying) credential, and just as importantly, what knowledge cannot be learned. Such specifications are needed for clarifying the interactions and trade-offs between security and privacy.

(iii.) Being able to specify environment assumptions that impinge upon security and dependability. This would include being able to specify the properties required by "out-of-band" procedures.

Pieter Hartel, University of Twente

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

The key challenge is to structure these emerging ICT environments by aligning them with the real world. At the same time, the real world will evolve as a result of new ICT becoming ubiquitous, thus making the real world something of a moving target. To achieve this alignment, the future Internet, an Internet of things, and any non-Internet based distributed systems (particularly WSN, WSAN) should have ingrained notions of *identity*, *time*, and *location*, supported by an appropriate architecture, algorithms and protocols of the network and its end-points. Without notions of identity, time, and location it will not be cost effective to prevent/avoid/detect/resolve the "tussles" that naturally arise when people use these emerging ICT environments for real.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

Technical measures dealing with tussles must comply with the local legal and regulatory frameworks, and do justice to the local culture and ethics. It will be a huge challenge to achieve the right balance between profitable businesses, effective law enforcement, and the users being in control of their own destiny.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

In view of the large variety of legal and regulatory frameworks, as well as the range of cultures and ethical value world wide, trans-national test beds are required to ensure that any new technology will be viable.

US/EU testbeds would be an excellent starting point.

Richard Kemmerer, University of California at Santa Barbara

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

(i.) Service-oriented architectures (SOAs) enable the dynamic integration of services implemented on heterogeneous computer systems. An advantage of SOAs is that they provide high-level, semantically-rich services by abstracting the low-level details of their implementation. However, what is needed is a comprehensive approach to trust modelling in SOAs.

(ii.) One challenge is that there is no agreement on what trust properties are, and there are no formal models of trust properties.

(iii.) Another challenge is that trust needs to be continuously managed along with other supporting components, such as operating systems, compilers, firmware, and hardware.

(iv.) There is currently no rigorous framework for ensuring trust all the way down to the hardware.

(v.) There is also a need for a rigorous approach to ensuring trust of the overall system, or workflow, when composing trusted services. How can one guarantee that composing services that each satisfy a particular trust property, such as privacy or resiliency, will produce a workflow that satisfies these properties.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

(i.) We need rigorous definitions of trust properties, formal models of the properties, and a formal framework for ensuring these properties. Even if there were agreement on trust properties; e.g., security, reliability, dependability, and fault-tolerance, new trust properties are likely to arise. Therefore, the framework needs to be extensible.

(ii.) Some trust properties can be ensured by using static techniques that can be applied to the services before they are put into use. Others can only be ensured at runtime, or it may be the case that a new service needs to be employed before it can be statically analyzed. For these cases, one needs architectural support for dynamically monitoring trust properties of untrusted services.

(iii.) We also need to develop a formal framework for trust management in SOAs. The framework would leverage automated verification and static analysis techniques that build on the modular analysis of individual services. These techniques and the resulting tools would address all levels of the SOA infrastructure, establishing a "chain of trust" from high-level models of trust to the underlying hardware resources.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

Need real-world example applications to evaluate the effectiveness of the trust management framework.

George Kesidis, Pennsylvania State University

In general, I think that EU-US cooperation can be effectively promoted with a streamlined system of travel grants to supplement existing and related proposals held by EU and US researchers. For example, if I want to visit a colleague in Paris for a week to collaborate with him/her on research funded by an existing NSF grant, I could apply for a travel grant (say a 1-page proposal outlining the planned collaboration, the value-add to my existing grant, and a little budget) with my NSF program manager. I

think that joint awarding of major research proposals is too complicated. A small pot of money could be set aside for this travel purpose. Testbeds such as PlanetLab naturally span national boundaries and Emulabs can be installed anywhere and remotely logged into. Finally, information sharing (esp. trace data) can facilitate cooperation.

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

In the future, S&D may need to be specified for a secure peer-to-peer overlay environment wherein fundamental problems such as anti-spam and secure routing may be quite different than those facing today's Internet.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

If the traffic in play is not sensitive to transmission-delay, then the S&D problem is not very different from the legacy problem of information assurance (over the Internet). If the traffic in play is delay sensitive and loss sensitive, then the S&D problem combines with the problem of achieving delay performance over the Internet.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

I think that the existing Emulab test bed (actually, a joint emulation and parallel simulation test bed), federated with PlanetLab is the right architecture. In some ways, an overlay test bed is much simpler in scope. Datasets specific to the application under test are generated by the experimenter. Background traffic is generated by emulated devices and otherwise "worst-case" background/attack traffic can be injected; to help with the latter, a repository of past attack traffic profiles can be compiled and made freely available to researchers. It's a mistake to build another test bed without frankly taking stock of the successes and limitations of existing testbeds.

David Kotz, Dartmouth College

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

(i.) Recognizing that the underlying "post-IP, post-3G" networks will provide a different security and trust foundation for S&D systems and applications - although a major challenge, we also still have an opportunity to influence these new networks to provide a better foundation for security and dependability. Since these new networks will be global in scope, this new foundation must be developed through international cooperation.

(ii.) The scale of future ICT environments may be small - a few isolated networked peers inside a car or home, with intermittent access to global services - or huge - millions or interconnected embedded sensors and actuators in a factory or power plant. A key challenge is to understand how to support S&D properties effectively and efficiently at many different scales. An international perspective is required to explore global-scale opportunities.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

(i.) Identifying applications, and application requirements, in a clear and consistent way so that the designers of the underlying networks and systems may identify the S&D tradeoffs and make informed

decisions about those tradeoffs. An international perspective is required to recognize applications that serve different national or cultural needs.

(ii.) Understanding the social, cultural, and legal foundations for security, privacy, and trust, as they relate to these applications. An international perspective is clearly essential here.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

(i.) We need "test beds" that support the interdisciplinary research on the applications and sociology of future ICT environments, with an emphasis on the S&D challenges. Some of the "smart homes" deployed already provide one example.

(ii.) We need data sets that allow ICT researchers to extract information, develop models, or drive simulations of future protocols and systems. Cooperative data-set collections provide a key foundation for the research community, providing common data sets upon which many researchers may explore ideas and compare their results.

Eric Luiijf, TNO Defence, Security and Safety

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

(i.) *Federation of independent secure systems* (at large), each having their own dynamic security policy. For example, DHS agencies who need to collaborate with EU agencies where there is only partial trust; network-enabled-capability; critical infrastructure owners connecting with each other and with governments/agencies.

(ii.) *Electronic trust in heterogeneous user environments* and *trust cascading* (friend a friend)

(iii.) Standards for applications becoming aware of QoS and bandwidth limitations, thus taking care of availability and resilience of *disadvantaged networks*

(iv.) Security architectures that allow *subcontracted technological security services* with third parties (or neighbour watch)

(v.) Methodologies to move away from static accreditation to *dynamic risk assessment and risk management* (dynamic security accreditation)

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

(i.) *Electronic trust*

(ii.) A unified way to *describe security policy* (XML-based; developing security ontology)

(iii.) Cross-domain *security policy negotiation mechanisms* and trusted cross-domain / cross Federation-of-Systems *security policy enforcement mechanisms*

(iv.) *Automatic transformation* from high-level security policies to component parameters while keeping them understandable for audit purposes

(v.) *Dynamic assessment of vulnerabilities* in a federation of systems

(vi.) A *common operational picture* of security posture and vulnerabilities in a federation of systems

(vii.) Improved *meshed PKI* technologies which removes the risk of a single-point-of-failure

(viii.) Development of *Policy-based Authorisation and Access Mechanisms*

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

Roy Maxion, Carnegie Mellon University

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

Metrics. This is key. Not much progress will be measurably achieved without metrics.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

We need an analysis of the key problems we have now, so that we don't bring along current baggage into the future.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

I don't know what testbeds and data sets we need, but I do know that these things are better decided by knowing what problem the testbeds and data sets are expected to solve. I also know that in the security world, people are not prone to the kind of detail that rigorous experimentation requires, and until that issue is solved, one wonders about the benefit of extensive testbeds and data sets. I also know that simply providing a lot of undocumented (or inadequately documented) data will probably cause more problems that it solves. In addition, bad data are worse than no data at all, because people will draw conclusions on the basis of whatever data they have (bad or not), and the entire community will accept these possibly erroneous conclusions. The community does not have a history of good judgement when it comes to data sets and to determining what constitutes quality data, or to what the consequences are of using bad data.

Takashi Nanya, University of Tokyo

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

A key challenge is, first, to define a set of metrics that can represent the degree of dependability and security from user's point of view for services provided by such unstructured and unbounded ICT environment at the end-user interface so that the value of dependability can be made visible and mapped to economic values, and then, to specify the design goal of each level of system hierarchy so that the S&D specification at the top level is reduced consistently to the lower-level design specification.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

The distinction between public services and private services must be modelled and characterized in order to appropriately evaluate and validate the value of dependability and security with cost issues being taken account of.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

Research on quantitative evaluation requires to take not only established research approaches for identification of the set of metrics, and for methods of measurement, calculation, validation, evaluation, but also interdisciplinary approaches where the evaluation results for user-level services are made visible and get mapped to economic values.

The latter approach may well be taken with international, both industrial and academic, collaborations toward global standards.

András Pataricza, Budapest University of Technology and Economics

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

If we look at the solutions offered by the professional IT providers, the try to reduce the nearly chaotic evolution by offering professional solutions in a ready to use form (service oriented architectures, and the evolving "software as a service" trend. On the design side the rapid spread of the model driven development is more and more supported by design intelligence (for instance, design patterns corresponding to the best practice) and high level runtime environments reducing the programming and deployment efforts (like BPEL).

One of the core problems is that development focuses primarily on increasing the scope and functionality is provided to the user, some standard do exist for the development process, but guarantees for the security and dependability guarantees does not belong to a well established common sense in IT provisioning. Frequently, users accept the consequences of security and dependability gets with a similar resignation, as those originating in natural catastrophes.

In some important advances follow a rather ad-hoc approach. For instance, the recent practice of creating service level agreements is typically done in a heuristic way. Small and medium enterprises usually do not comply with such fundamental initiative like ITIL.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

Security and dependability had to be integrated into or the aspects of the design and execution workflow. This necessitates the close integration of model based design methodologies with formal methods based proof of dependability and security compliance, the creation of similar platforms for the individual application domains, like the Service Availability Forum addresses them, and a model based design methodology for system and service monitoring and management integrated into the application workflow.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

At least the academic community has very little input from real life experiences, as fault and security related data are mostly confidential to service and product providers. This way, the academic world would need more orientation from the real life statistics. The dominant fault models, their occurrence rates are fundamental to orient and motivate further research.

Vern Paxson, Lawrence Berkeley National Laboratory

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

The three very large challenges I see looming are (1) the struggle over control of the content of communications conducted using future networks, (2) varying legal and policy issues regarding such usage, and (3) the degree to which the utility of such internetworking rests on the rich semantics of communication vs. the difficulty/un-decidability of third parties (to the communication) being able to discern these semantics. All three of these inter-relate.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

Per the above, the key struggle concerns the ability of third parties to understand/control/modify the semantics of the communication enabled by future networks. Sometimes these third parties are as simple as defensive software running on end-hosts; but other times they are potentially antagonistic separate entities such as network providers whose interests do not align with those of end users.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

I am sceptical of the ability for test beds or models to capture the rich and sometimes quite peculiar semantics present in actual communication. This leaves data sets, and the very difficult problem of how for research purposes to observe the full semantics of communication without potentially deep risks to end-user privacy or security.

Michel Riguidel, École Nationale Supérieure des Télécommunications

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

The following areas are identified as research challenges:

(i.) *Ambient security, dependability and privacy.* The mass diffusion of digital systems must be endorsed with built-in mechanisms for enhancing confidence in their usage. The following main issues need to be tackled:

- Networking aspects: Common security mechanisms mainly based on boundaries and firewall protection mechanisms do not scale with regard to new complex systems. We should imagine different mechanisms such as those based on analogies with the bio-living world, (e.g., immune and self-healing systems), as well as autonomic, evolvable and adaptive security mechanisms. This will definitely require new cognitive techniques and semantic models managing the complexity of ambients where people/devices may jointly act and interact.
- Security for small devices: Security systems and cryptographic mechanisms must be scaled down in order to be inserted in small devices (even at nano-scale). Tiny devices will definitely have specific requirements such as energy consumption, computation power, and so forth. Efficient, flexible and scalable low-cost cryptographic protocols and mechanisms must be developed and combined in order to create a secure and dependable Ambient Intelligence space as well as ensure privacy protection.
- Secure and dependable software: We need also to develop a discipline of system and software security based on the development of methods, tools, and repositories for high-level verifiably secure programming. We advocate an approach based on efficiently verifiable mathematical

proofs showing compliance to policies, expressing safety, security, dependability or functionality constraints.

- Assessability: Finally, we need mechanisms and tools for assessing and proving the security and dependability of a complex system. During the last years, many techniques have been developed, especially in the dependability community. Yet, the scale of new ICT systems and the kind of threats and assumptions on their operational environment (not last the human factor) pose new challenges and the need for an assessability discipline is even more impelling. Different metrics, modelling tools and observation mechanisms are needed. The capability of measuring the tolerance to attacks is crucial in new systems that due to their logical and physical diffusion are likely to be under constant attack.

(ii.) *Dynamicity of Trust.* The lack of trust is one of the main barriers for the establishment of a secure and dependable Information Society. This can be a lack of trust in the cyber-infrastructure, due to frequent attacks or fears about the design of digital systems, but also includes the difficulty in modelling trust relationships among digital entities, and between humans and digital entities. Future ICT systems will involve thousands of millions of devices (including nomadic devices), as well as virtual entities (such as Virtual Private Networks and Overlay Networks), and will no longer be able to depend on setting boundaries and firewalls for their security. Instead, they will require a capability for managing and negotiating trust relationships, adapted to the level of security required in a given situation. The understanding on how trust emerges and evolves as well as of related notions as reputation formation, monitoring and evolution are mandatory. The challenge is then to obtain a greater understanding of partial trust, security-based trust (where trust follows from security), and trust-based security (where security is achieved through a trusted partnership), and to use this understanding to realise a high level of trust of the citizen in the deployment, economic viability and social acceptance of systems and services. This will require expertise and joint research in several fields outside ICT, such as economy and sociology.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

Future ICT systems will have to cope with the following key characteristics:

- Complexity – as hardware capabilities improve and costs reduce, there is continuing pressure to attempt to build systems of ever greater scope and functional sophistication, especially for the software components and for the virtual paradigms;
- Multiple innovative types of networking architectures and strategies for sharing resources – GRID-like, peer-to-peer, "on-the-fly" services, overlay networks, virtual architectures, etc.;
- Boundary-less nature of the systems and interconnectedness – few systems have a clear-cut frontier, and they are drawn in systems within systems; in addition all nodes, connected through a common underpinning infrastructure that becomes a critical factor, are potentially accessible from anywhere anytime, which results in unpredictable emergent behaviours;
- Heterogeneity and blurring of human/device boundary – wrist-held gadgets, wearable devices, implantable devices; bio-digital interfaces;
- Incremental development and deployment – systems are never finished, evolution is incessant, upgrades, changes in functionality, new features are being added at a continuous pace; systems are expected to be able to respond to the changing circumstances of the ambient where they are embedded;
- Nano-scale (operating) systems will need usual ICT features to be scaled down so that they can be implemented in such systems.
- Multiplicity of fault and attack types – in particular the growing danger of malicious faults, both due to individual or organised external attackers, and due to deceitful insiders;

- Massive dissemination of digital traces representing behavioural, personal and even biological information (as DNA, fingerprints, etc…);
- Online services; security of software updates or downloading, distribution of multimedia contents, distribution of digital services;
- Mobility: nomadicity end users, mobility of infrastructures, virtual overlay networks.

The scale, complexity and ever-expanding scope of human activity within this new ecosystem present enormous technical challenges for system security, resilience, dependability and privacy. We currently lack both a conceptual framework and adequate tools to resolve these problems. There is a need to model and understand the multiple interactions and interconnections (human, technical, social, market) among systems, when they all depend on each other. The ecology of these interactions and interconnections needs to be addressed through analysis and techniques for security, dependability and privacy.

Traditional security models based on a rigid perimeter defence have failed as they are based on assumptions of closed tightly controlled networks that no longer apply. Future pervasive ICT with billions of networked devices demands a new paradigm shift towards self-organising, self-healing and self-protection systems. Such a paradigm could benefit from bio-living world inspiration where such organized communities/populations exist and evolve.

We need also to consider efficient, flexible, robust, and scalable low-cost cryptographic protocols that allow building up trusted channels and services by combining cryptographic means with other information (location, neighbours, reputation,) and that manage to combine privacy protection with personalization. This will require novel cryptographic technologies relying on efficient instantiations and evolutions of several security protocols, in particular the secure multiparty computation protocols. Systems will need to offer features such as personalization and smooth interaction with users, but users will also expect that these systems are robust and reliable, and offer an individual or community "sphere" which offers protection and privacy. One can offer these features by building on strong security properties of the components or of a set of tiny subcomponents – they need to offer a series of features as authentication or anonymity, secure data storage or data matching or exchange, and trusted execution.

Given the increasing complexity and distributed nature of systems, we will also need to consider the development of methodologies, languages, tools, and standards that facilitate interoperability and integration, and generalize deployment scenarios such as remote maintenance of devices. At the same time, the need for secure code will become more prominent, because the distinction between applications and systems will gradually disappear and most code will have consequences for security. In this respect, the task of writing secure code is becoming tremendously more difficult, because of the lack of effective support to integrate security considerations in system development.

A main requirement for all engineered systems is the ability to assess their ability to function properly and the quality of service that they will deliver under both normal and stressful conditions. This is an essential ability at all stages: for designers to decide among alternative architectures, for parties in contracts to decide on prices and conditions they will accept, for owners to decide on procuring, abandoning or overhauling their systems, for policy makers to decide on their acceptability for society or on proper legal or regulatory regimes. Some of these assessment activities have to depend on a priori knowledge and can be conducted during design, some can or must rely on observing the system in testing or actual operation. Eventually, in pervasive systems, adaptation and evolution will depend on continuous automated assessment.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

Test beds are networking testbeds to evaluate and validate the following points:

(i.)Networking aspects

- Understanding new risks and threats arising from the dynamic and evolutionary nature of the systems and their environments and developing methods for user-oriented risk assessment;
- Understanding the boundary-less nature of systems and their failure behaviour with a need for modelling, data collection, experimentation, assessing systemic risks, and the possibility of emergent behaviour and surprise;
- Developing security, dependability and privacy protection technologies to deal with increased scale and complexity and criticality (telecoms, embedded, smart cards) – emphasis on critical components;
- Developing self-healing and self-organising capabilities into the ambient computing space. Specifically algorithms need to run at every node and communication protocols are required to bind the resulting heterogeneous systems into a cohesive unit, that is also dynamically stable (since self* processes can follow local optimization rules, that are globally conflicting);
- Understanding where the boundary between autonomous system defence and human intervention will reside; this will be a dynamic interplay as both technology and legal/social policy both co-evolve;
- Developing system architectures for large-scale networks using techniques for autonomous administrative roles and system management as well as defining policy models for autonomous software, e.g. multi-agent systems;
- Designing resilience, security, dependability and privacy in new networks and systems to come (Future Internet, Internet of Things, post-3G telecom infrastructures, post-IP networks): complete new design in security and dependability of protocols which will be embedded in future communication infrastructures, replacing current Internet Protocol suites (IPv4 or IPv6, TCP, SSL, SIP, etc.)

(ii.) Security for small devices:

- Developing low-cost and low-footprint building blocks and developing a methodology for assembling these building blocks so that security properties emerge at the system level even if the building blocks are not perfect;
- Developing methods for modelling, building and evaluating secure implementations of cryptographic algorithms, protocols, middleware, operating systems and applications at the small scale, and even at the nano-scale.

(iii.) Secure and dependable Software:

- Developing foundations for secure software: developing methods, tools, and repositories to help developers analyze security implications of their code, and more generally to develop verifiably secure software.
- Developing tools and infrastructure that will guarantee to end users that the software (to be) installed on the systems they use is secure through verifiable evidence.

(iv.) Secure delivery of digital content

- Developing methods for modelling, building and evaluating secure distributions of content delivery along the whole trust chain of players (creators, editors, distributors, providers, end users), protocols, middleware and applications: watermarking, IPR (Intellectual Property Rights), Digital Rights Management (DRM), harmonization.

Reijo Savola, VTT Technical Research Centre of Finland

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

(i.) Prioritized technical issues to address over the next 3 years:

1. Threat & attack analysis
2. Specification of highly converged systems and networks
3. Definition and prioritization of security requirements

(ii.) Suggested mechanisms to establish EU-US co-operation:

- Aggregation of state-of-the-art knowledge
- Co-funded research projects with case examples from industry (both EU and US)

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

(i.) Prioritized technical issues to address over the next 3 years:

1. dynamic behaviour: self organization of networks and systems
2. identity management in the ubiquitous environment
3. key distribution

(ii.) Suggested mechanisms to establish EU-US co-operation:

- Aggregation of state-of-the-art knowledge
- Co-funded research projects with case examples from industry (both EU and US)

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

(i.) Prioritized technical issues to address over the next 3 years:

1. threat and attack models (models of negative behaviour)
2. structured security metrics
3. trust and reputation models

(ii.) Suggested mechanisms to establish EU-US co-operation:

- Aggregation of state-of-the-art knowledge
- Co-funded research projects with case examples from industry (both EU and US)

Jason Smith, Queensland University of Technology

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

The selection of an appropriate level of abstraction (or abstractions) for such specifications, would appear to be a significant challenge.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

(i.) Significant challenges associated with run-time security versus designing security in. Presumably, the components (or a subset of components) within polymorphic MME's will be required to exhibit certain security and dependability properties. How will the minimum number of trustworthy components required to construct a trustworthy service be determined. How will the service user (or provider) detect when the number of components required falls below a minimum threshold and how will they react?

(ii.) Deciding where service intelligence lies (in the network or in the end points) and how this intelligence might migrate between the two, depending on context. Quality of service and denial of

service resistance would seem to require intelligence in the infrastructure. Resilience and fault tolerance, intelligence in the end hosts. But in emerging MMEs, limited assumptions can be made as to the capability of end hosts, as they may be disposable, lightweight devices.

(iii.) Determining how intelligence should migrate between the edge and the core and the instantiation of this (virtualization??) will require advances in trusted systems technologies. Gaining assurance that such approaches can not be used against the system (via denial of service attacks for example) may be problematic.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

On the assumption that some subset of components in future polymorphic networks must exhibit predictable properties, how can assurance of such properties be obtained? The scale of the systems involved would make current approaches to evaluation infeasible. Furthermore, the timeframes for evaluations are far too long to remain relevant to the dynamic nature of these emerging, unbounded infrastructures.

The dynamic nature of service provision, and the extensive use of proprietary underlying technology suggests a need for improved techniques for evaluating and assessing, in a black box fashion, the runtime behaviours of components, systems, and services. Such challenges would seem to be present not only in future networks, but emerging areas such as dynamically composed web services.

Assuming future networks are an order of magnitude greater in scale and contain highly heterogeneous components and technologies, efficient techniques will need to be developed for the evaluation of large, and most likely highly distributed, data sources. How can these data sets be efficiently distributed / accessed? How will access to such data sets be secured to ensure that the information contained within them cannot be used to undermine the S&D of the infrastructure.

Neeraj Suri, Technische Universität Darmstadt

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

(i.) Specifying the dimensions (computing/communication heterogeneity; mobility, density; policies, power, storage, ...)of the MME!!! The dilemmas arise as the needs for desired functionality dictate increasing dimensions and interactions; On the other hand S&D works best with bound/control on the interactions. With functionality dictating the design of future ICT, S&D needs a re-think from the current 'system' view to a 'services' view

(ii.) Meaningful scoping of an 'adaptive' environment, i.e, what are the building blocks and interfaces that result in (a) scoping and (b) partial structure of the unstructured environment

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

(i.) The 'service' model for protocols where deterministic S&D delivery is probably a hard expectation while QoS in S&D is as fuzzy as it sounds.

(ii.) Semantics and metrics for S&D. Need to keep in mind that its S+D not S,D

(iii.) Scalability & composability of S&D attributes gives that S&D are mostly non-composable

(iv.) Understanding the trade-off across MME opportunities (potential high resource access) vs. MEE constraints (eg. determinism/guarantees are perhaps elusive here)

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

(i.) Testbeds characterizing the varied dimensions of the MME. Deployment, load/behaviour characterization, scaling, validation... TU Darmstadt is setting up a large scale (campus wide) MME WSN under a German National contract - that is potentially available to the research community at large.

Wade Trappe, Rutgers University

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

(i.) *Predicting the Shape of ICT and Threats:* The future ICT will involve new ways to use the communication infrastructure. Currently, we are used to thinking about "humans using the Internet" where the security problems are tightly tied to the identity of the human (e.g. electronic commerce). Moving forward, there will be new devices, new programs, new applications that won't resemble what we are used to, and for which we might not even be able to predict. The new and unpredictable shape of ICT also means that the shape of its threats will be hard to predict. Already, we have seen this with botnets—who would have foreseen their existence?

(ii.) *Scale:* There will be an ever increasing amount of devices on the future ICT. Architectures are being developed to allow more devices to be networked, from refrigerators that can surf the web to sensors in automobiles that report measurements to a monitoring service. As everything around us becomes networkable and compute-capable, we now face the fact that everything can become a platform for attack.

(iii.) *Lack of Awareness on the Part of Industry to Adopt Security:* Security usually has a stigma associated with it, and often companies are in a rush to "get to market first rather then get to market best". The result is that security is often avoided or not considered until after a product has a firm foot hold. We have seen this with WiFi (luckily the security flaws are being fixed), and we have seen this with electronic voting systems (where the flaws are not really being fixed).

(iv.) *EU-US Mechanisms for Co-Operation:* One of the most basic ways to reign in the potential reckless abandon, by which technologies are being created, is to specify standards. To many, standards are good and to many standards are bad (hinders differentiation and competition). However, the need for some form of common guidelines (i.e. recommendations, not necessarily standards) that technologies should strive to adhere to would be beneficial. Perhaps an ideal form for this would be to create a commission/think-tank where individuals produce whitepapers with S&D guidelines for different applications domains, or whitepapers that identify common requirements across different technologies. (To give an example, two application areas that are solely lacking in S&D guidelines are RFID systems and SCADA systems. There are definite commonalities, but neither has a standards community savvy in security). Finally, this organization needs to have a strong public relations presence: whitepapers are only useful if they are read and their knowledge is disseminated.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

(i.) *Identity versus entity:* As noted above, the human might not be as relevant in the future. Securing human applications involves tying things to individual identity. However, many of the processes running on the future network will not involve humans, but will involve a broader arrange of possible forms—from RFIDs and sensors to wireless handheld devices to entertainment systems. Many of these entities might not have a "Layer-7 (Application Layer)" per se, but instead may serve lower-

layer functions (either as its sole function, or part of a greater collaborative communication infrastructure). In this case, security paradigms might increasingly need to isolate a "transmitter".

(ii.) *Identity reuse:* Even though there will be many applications where the human is not involved, there will be more opportunities for the individual to interact with more services. As a result, the individual will likely have to have security relationships with many organizations. As a result, the individual will likely reuse passwords, etc. in order to make life easier for him/herself.

(iii.) *EU-US Mechanisms for Co-Operation:* As above, I think that the formation of a think-tank organization to identify requirements is important, and would help specify potential architectures as well.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

(i.) *We need testbeds that people outside of academia use for development and security testing!* Currently, DETER, Planetlab, ORBIT, EMULAB, and KANSEI are used for producing academic papers (admittedly, there might be some corporate usage, such as on ORBIT, but these projects are typically not security-related). How to get these testbeds used for security evaluation is problematic.

(ii.) *Data sets might be a bit "after-the-fact".* It implies that technology already exists, some protocol is already running, and data is being collected on the operation of that technology. This means that the role of data sets is probably primarily in "diagnosis" and patching, rather than in development of the initial technology.

(iii.) *EU-US Mechanisms for Co-Operation:* The EU-US should encourage security research and development on these "public" testbeds. It should be noted that isolated testbeds do not allow for verifiability. Perhaps one idea for co-operation between the EU and US is to create a consortium of testbeds and identify cases where test bed duplication and global distribution might be needed.

Alfonso Valdes, SRI International

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

Poorly understood and specified interfaces permit information leakage. Coupled with weak authentication, this raises issues of identity management and privacy as people go through their digital day, and presents a formidable barrier to realization of the economic efficiencies enabled by pervasive diverse communications. Moreover, the opportunity for fraudulent financial gain and falsification of false identities provides significant benefit to organized crime and terrorist groups.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

How does one authenticate to a multitude of one's own devices (usability issue)? How does one authenticate to conduct transactions (a Bluetooth phone authenticates to an IP enabled vending machine)? What data is it appropriate to retain, and for how long? How do we safeguard this data so that only the appropriate data is revealed to constitutional authorities for forensic purposes? How do we address issues of cross-border communications?

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

Test beds, data sets, and models must comprehend massive scale, heterogeneity of sources, and diverse international standards and policies.

Jody Westby, Global Cyber Risk, LLC

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

Legal and policy issues will prove to be more difficult than the technical issues. The international legal framework around privacy and security is highly complex and inconsistent. There are no greater gaps than that between the US and EU privacy legal frameworks and the cultural perceptions about what data governments should have access to. For example, EU citizens generally feel safe letting their government have whatever information they need about them, but they are very untrusting of private sector entities collecting the same data. In the U.S., it is just the opposite: U.S. citizens do not generally care about what information private sector entities have about them, but they are paranoid regarding what data the government may collect. Tensions are especially high if private sector entities begin sharing their data with government agencies, especially law enforcement.

There is also great disparity in international cooperation of law enforcement, investigation of cyber-crimes internationally, and criminal procedures governing search and seizure, wiretaps, and access to stored electronic data. The Council of Europe Convention on Cyber-crime was mirrored in the EU Council Framework Decision on attacks against information systems, and the US ratified the CoE Convention. We are a long way from a harmonized approach to these issues, however, since every country that is a Member of the EU or a signatory of the Convention has to implement the Convention or Framework Decision into national law. This takes time and the jurisdictional, procedural, administrative, and legal differences will continue to stymie and hamper S&D efforts. It is for this reason that a multidisciplinary approach to these problems is essential. Legal, technical, and operational viewpoints must converge.

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

I don't think I am qualified to answer this question.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

Test environments must include realistic traffic data and test networks. The traffic data will be a problem due to varying privacy laws around the globe. Serious efforts must be undertaken comparable to those that Doug Maughan has included in his PREDICT project to ensure that privacy considerations are seriously addressed, that privacy impact assessments are written, and that meaningful dialogue with the privacy community is undertaken and sustained.

Theme 2: Attributes and Mechanisms for future Distributed Services and future Overlay Networks and Applications

Michael Bailey, University of Michigan

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

(i) *Identity and membership.* Understanding identity in the context of today's Internet is a complex problem whose limitations has hampered solutions to numerous important S&D problems (e.g., SPAM, Denial of Service attacks). In future ICT systems assessing and assigned the notion of identity becomes even more complex. Understanding what we mean by identity (e.g., device identity, application identity, user identity, host identity, AS-level) and validating these identities without a centralized or fixed trusted source, while still maintaining the privacy of the individual user is a daunting task.

(ii) *Capabilities and context.* While identity and membership are properties of the user or group, capabilities and context are the properties of the mixed infrastructure, devices and application environments in which the user find herself. Establishing these capabilities is key to building effective applications and defining the roles a device or user may play. These attributes may extend beyond simple bandwidth, latency, memory, etc. to notions of trusted or untrusted environments or changing roles of individual users in a system. These attributes may be used to define the types of data the user may access or store given the current contextual role or physical connectivity attributes (e.g., you may not read email in an untrusted environment, unless encryption capabilities exist).

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

(i) *Policy enforcement.* As the user's identity and capabilities are increasingly fluid in heterogeneous and polymorphic ICT systems, the ability of administrators and users to define effective policy for applications and data becomes increasingly difficult. In order to be effective at assuring the S&D dependability of these systems administrators need the ability to specify fine grain data access and network utilization policy, possibly at the level of per user, per device, and per file/object. This policy enforcement must be ubiquitous. It must move beyond the traditional walled fortress approaches and include not only enforcement across organizations, but also within the various departments, buildings, floors, and groups that make up each organization.

(ii) *Virtual networks or trust communities.* In order to solve S&D issues in tomorrow's ICT systems, we will require methods to seamlessly and effectively establish trust and share information across different entities. Unfortunately the Internet today is akin so a collection of loosely coupled city-states. Each organization has its own policies and detection and enforcement mechanisms and some organizations may have completely opposing policies. Future ICT systems are likely to be even more heterogeneous. To facilitate sharing of information and unified policy enforcement future ICT systems should support methods for building trusted network communities and virtual networks consisting of users/nodes/machines with similar properties and with whom a level of trust has been established.

(iii) *Measurement and auditing.* Measurement and auditing of the various user and environmental attributes as well as the performance and behaviour of the mechanisms which are created is essential

for the effective validation of these systems. Measurement methodologies in today's networks make use of grafted or overloaded technologies (e.g., Netflow was designed for accounting not traffic characterization) in order to estimate the effectiveness of various protocols and applications. To overcome the limitations apparent in today's network monitoring (e.g., too much or too little data, trustworthiness) new ICT system should build monitoring and auditing as first class citizens and include reasonable support of these activities (e.g., support for triggers and hooks inside protocols, scalable deep packet inspection).

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

(i) *Threat models.* Because there is little hope we can predict the actual exploits likely to exist in the next generation protocols and applications, the key way in which we will be able to assess the S&D of future ICT systems will be in the generation of realistic threat models. Looking to existing trends in attack targets and exploit methods in combination with an assessment of new capabilities will be required to accurately characterize the likely means and motives of future attackers.

(ii) *Usability.* Key to understanding the effectiveness of these new applications built on the methods defined here is the ability to measure their usability and adoption. It is clear that the weakest link in the security and dependability of existing systems is the end user. For example, it is a mistake in configuration has resulted in the largest Internet outage to date. Email-propagation and spyware / rootkits installed with user's consent (if not explicit knowledge) are fast becoming the most important infection vector in existing systems. As the number, types, and complexity of these network systems and applications increase, understanding the ease at which these systems allow users to specify policy and assess risk is important.

(iii) *Real world testbeds and datasets.* Again I emphasize the idea that the testbeds and datasets used to drive them must solve the limitations of existing modelling and simulation environments. They must involve at scale infrastructures and be driven by real user inputs or datasets derived directly from them to be effective.

Sandro Bologna, ENEA

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

What is needed is a multi-layer modelling capability (physical layer, logical layer, human and organizational layer) and their interactions. Attributes will be different for the different layers (e.g. at physical layer failure rate of components and level of redundancy, at logical layer number of software errors or virus infections reported, at organizational layer number of malicious intents reported). Most challenging is the possibility to link all these different modelling and/or attributes to be considered together.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

The test bed should make available a set of modelling tools spanning from topological modelling to stochastic modelling, Markov modelling, ….., cognitive modelling. How to link all these different types of modelling should be investigated.

Nikita Borisov, University of Illinois

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

The privacy requirements of current and future applications are still not well understood. For example, the issues of collection, access, and use all seem relevant to privacy, but solid models and policies addressing these issues are still emerging. Further, the cultural norms for privacy and cultural awareness of privacy issues linked with information technology are diverse and evolving. International collaboration for studying these norms and building corresponding models and policies seems essential.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

Current trends point towards networked services providing applications and managing users' data. The technical challenges in this space associated with security and privacy are how to manage data in such a way as to reduce the potential impact of failures, vulnerabilities, and insider attacks, and how to implement security and privacy policies in a verifiable way, to avoid creating a lemons marked in supposedly-secure networked applications.

Other challenges lie in implementing stronger isolation protections to enable more pervasive sharing of resources among organizations, and in addressing issues of regulatory compliance. Compliance research is an active area in both EU and US and joint efforts to address compliance are necessary due to different requirements and complementary experience across the nations.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

To evaluate technologies, we need:

- Models for regulation to verify compliance
- Surveys and description of privacy attitudes, priorities, and requirements across different cultures
- Models and data sets pertaining to sensitive information. Current research on preserving privacy of sensitive data relies either on very limited data sets, or on privacy-compromising data sets that have been accidentally released, such as the AOL search database. An effort to build a model with supporting data that can demonstrate what kinds of information are privacy-sensitive without compromising the privacy of the owners of the data (or violating privacy-protection legislation) would improve the state of the art in privacy research.

James Clarke, Waterford Institute of Technology

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

(i.) There are a number of Socio-technical challenges that needs to be addressed. Given that we are moving into an ubiquitous, mobile Information Society, with MME and continually evolving networked environments, the context for defining a new security paradigm in this new emerging Information Society is made very complex. The new security paradigm is distinguished by striking a reasonable balance between a Big Brother Society to a fully confident building and privacy and ethics protecting society (the Empowering the Stakeholder view as discussed at WS 1). The establishment of society's confidence in this new digital world requires the creation of a palpable defensive environment enabling citizens' control over the type and level of protection associated with the goods and services accessed or delivered through digital media. However, it must be clearly recognised that the means of providing this confidence should lie within an overall context of the citizens being able to live a free, unencumbered, comfortable and prosperous life: being protected against the risks of digital intrusion, crime, terrorism, etc., must not be seen as more of a burden than the risks themselves. In order to achieve this, ICT trust, security and dependability will need to become a matter of routine, and not be a source of potential problems and nuisance as often perceived today. Security and dependability will need to be a transparent, unobtrusive part of the operation of economic and social activity in a digital environment. To achieve this transparency, there needs to be a common taxonomy and terminology that is understood by all stakeholders. This will allow the development of a generalized, layered abstract model of security and dependability requirements and solutions that avoids the need for the users to know the detailed 'plumbing' of the underlying technologies.

(ii.) Federated identity management across these environments.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

(i.) There is a new world of the Internet, where boundaries are no longer clear and anyone can set up a network. To begin to deal with this situation, we need to build intelligence into networks so that rogue/malicious elements can be recognized and eliminated. Citizens must have this new Internet at their disposal with guarantees of privacy and confidentiality.

(ii.) There must be built in Monitoring for these systems to enable identification, study, prediction and prevention of re-occurrence of events. This should also encourage an approach whereby all stakeholders are involved in the examination of why or how a given system failure has happened. Specifically, there need to be approaches that:

- allow the determination of the extent to which the fault was human, some aspect of the system, or a component;
- enable a significant reduction in the probability that similar incidents will occur again;
- allow cross disciplinary investigation of incidents, including sociologists and other related disciplines;
- involve setting up a moderated global forum including all communities for sharing information of all aspects of network dependability and security.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

(i.) There were a number of test bed ideas raised and discussed at WS number 1 that I would like to see moved forward. An example of potential collaboration stems from the fact that the US side seems to have more facilities concentrating on the lower level (network) whereas in the EU, there is more concentration on the higher levels (services, applications). Therefore, the communities should leverage this synergy, for example, by establishing an application and software services test bed that could be built on top of GENI with a number of application level experiments. Planetlab runs a

production level services platform and University of Berkeley is also building an experiments cluster, which may also be used for this purpose. It was recognised that there would be a significant amount of collaboration required as the middle layers, which provides the OS would need to be jointly addressed also. The underlying rationale for the establishment of this test bed was that the current experimental facilities, although open for unlimited experimentation, the focus is on network innovation. Therefore, it is left to the one's who want to run the experiment to set up from scratch the application, software and service environment. For SOA, this is not feasible for most especially SMEs and Academics. Therefore, if there was a software and services test bed 'playground' already set up, this would open up tremendous opportunities for others including innovative SMEs and academics to venture into service-oriented solutions, without having to endure the expense and complexities of setting up a full scale test bed.

(ii.) Another test bed discussed was one for wireless or sensor networks. There are some standalone test beds already available but the issue that must be explored is to how to federate them taking into account cross testing, mobility aspects and security policy's as user's move in and out of different environments.

(iii.) Regarding the mutual necessity and benefits of global co-operation that would justify and motivate the practicalities in establishing the co-operations with these particular answers, I believe they fit the categories because of the synergy expressed above for future testbeds and also for the socio elements raised, it will be necessary to work on these together in a global way in order to get it right the first time. We are also aware that the US side is also looking at the interdisciplinary approach similar to the EU side as expressed above in the socio elements answer to question a (reference: Institute for Security Technology Studies (ISTS) at Dartmouth College Newsletter Winter 2007) so this is an area we can work together.

Marc Dacier, Institut Eurecom

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

(i.) Several existing attributes are known and have been studied for a while. They certainly remain valid (confidentiality, integrity, availability, reliability, maintainability, etc.). We may want to consider new required attributes though for these systems to enforce expected S&D properties. An important one is adaptability. Systems may have to be able to reconfigure themselves, choose new security mechanisms, behave differently, as a response to modifications observed in a fast changing ICT environment. Without such ability, it may be impossible to enforce some S&D policies.

(ii.) The other new attribute that may get a growing importance in those systems is what I would call "acceptability" of S&D enabling techniques. S&D mechanisms must be built in such way that their impact on these environments is acceptable. This is true when looking at their deployment on embedded components but it is also true when considering the end users. The most secure solution is useless if the user decides not to use it either because he is not convinced of its usefulness, because it is to complicated or cumbersome to use, or even because he does not trust the solution to be harmless for other components or properties (e.g. he thinks it could degrade quality of service)

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

(i.) Building intrusion tolerant systems, i.e. accepting the idea that we cannot build systems where security failures can not be avoided, imposes on us to design methods and techniques to assess the ability of these new systems to deal with the failure of some components. This means that we can define, characterize, quantify, assess the various failures modes of the components, their rates, etc.. As long as failures are due to accidental causes, this is something we are used to do. However, if the causes are intentional and human made, the problem is completely different. We need to be able to understand, analyze, model the human actors behind the expected attacks, their modus operandi, etc..

Technically speaking, this requires two major challenges. First of all, we must gather enough material about real attacks to be able to derive models that could be used for predictive purposes. Second, as human beings are involved, we will have to take into account elements such as sociology, psychology, etc.. of the trouble makers. Such interaction requires interaction between research communities that, so far, have not vigorously cooperated together..

From an international perspective, it will be very interesting (read complicated) to see if models of the can, or not, be applied on a worldwide scale or if, at the contrary, they obey to local circumstances. In other words, it would be interesting to see if S&D of a system is, or not, a function of external contextual elements, such as the country it is residing in. If yes, it would also mean that S&D mechanisms may have to be adapted to cope with local conditions, whatever local means when considering the Internet.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

(i.) As explained before, there is a real need to have shared techniques and methods to capture meaningful, rich, quantitative and unbiased information about attacks on a worldwide scale in order to start analyzing thoroughly the problems that exist and those that are emerging or likely to emerge (e.g. attacks against routing protocols, be them the ones used today or the ones proposed for these new environments). We should also, whenever new ICT infrastructures emerge take that monitoring factor into account and have this ability embedded into it.

(ii.) International testbeds should be available to experiment with attack models and techniques.

Carl Gunter, University of Illinois

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

Sorry, I'll need to leave this one for the meeting. I'm not sure I understand the question. What is a "polymorphic" network? More intrinsic DoS protection would be a good target feature for a future version of the emerging Internet.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay /Infrastructure solutions, large and small scale security, long term security, middleware solutions?

I think one improvement in mechanisms would be protocols for the dynamic discovery and traversal of security gateways such as firewalls, address translators, and VPNs. Current solutions are too manual and there are no good mechanisms for learning and coordinating policies between domains.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

The answer for 1(a) seems equally important here.

Richard Kemmerer, University of California at Santa Barbara

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

In order to assure the security of future polymorphic networked systems we need total situation awareness. That is, we need to perceive what is going on in the environment (via intrusion detection alerts), comprehend what these alerts mean, and predict what is going to happen. The correlation work done by the intrusion detection community has provided the initial steps toward situation awareness by fusing, aggregating, and verifying alerts to help reduce the mass quantities of data that are produced by the intrusion detection systems. However, to better comprehend what is going on and to be able to predict what the adversaries' next moves may be, it is necessary to expand the current correlation approaches to include information about the missions being carried out, the status of the assets that these missions are dependent on, and the possible alternative courses of action (COAs).

(i.) A viable situation awareness solution for a large-scale cyber network needs to provide aids to understanding the current activities. More specifically, it is necessary to provide the infrastructure manager with a succinct picture of the adversarial activity on the cyber network being protected. The infrastructure manager also needs the capability to analyze the impact of the adversarial activities.

(ii.) Knowledge of what assets have been compromised or are being threatened is paramount to determining the proper course of action. The infrastructure manager also must have the ability to anticipate what is going to happen next.

Purely reactive solutions are not good enough; one needs to be able to predict future actions and proactively defend against them. The infrastructure manager should also have ready access to alternative responses to counter current and future attacks.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay /Infrastructure solutions, large and small scale security, long term security, middleware solutions?

There are a number of technical challenges that need to be overcome to build a situation awareness toolset that enables the infrastructure manager of a large-scale cyber network to reliably assess the impact of adversarial actions against the network and to predict future adversarial actions.

(i.) The amount of raw information produced by the many intrusion detection systems running on a large-scale cyber network is too large to be processed manually. Some form of correlation to verify and fuse the multitude of alerts is needed.

(ii.) It is impossible to understand the impact of an attack without knowing what critical assets were compromised and what their role in the mission is. Therefore, there is a need for a Mission Workflow Database (MWDB) and a Critical Asset Database (CADB). The MWDB contains cyber-missions, which are sets of low and high level tasks that must be performed in the specified order and within the specified time constraints to support the operational mission. A CADB keeps track of the computing resources (assets) that are needed to accomplish the tasks that comprise a mission.

(iii.) Tools to monitor the critical assets and to discover any asset dependencies that may have been missed when the CADB was generated are also needed. The CADB and MWDB also need to be integrated into the extended correlation process to provide a situation awareness tool suite that can determine the defence status of the network, the impact of the attacks on the current mission(s), and provide alternative courses of action to counter the attacks.

(iv.) To enable the infrastructure manager to better determine what countermeasures to put in place, it is helpful to have a means to formulate "what if" queries that help understand the impact that either future attacks or different responses would have on the cyber-mission.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

Test beds where large, complex attacks can be simulated would be very useful.

George Kesidis, Pennsylvania State University

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

At once more sophisticated and scalable models of federated, hierarchical trust need to be developed and hardened. These trust systems can be applied to many S&D problems if they themselves are secure.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

Further research in experimental methodology is required, especially to deal with artifacts and limitations of testbeds, so as to yield more compelling experimental results. This is especially so in a peer-to-peer environment.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

See my general comments for Theme 1.

David Kotz, Dartmouth College

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

I'm not sure what you mean by attributes. Here are some key attributes of a successful solution; 1. Usability 2. Simplicity 3. Flexibility and Expressiveness 4. Scalability

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

(i.) We need a usable, scalable, flexible, and deployable public-key infrastructure. That infrastructure needs to work with small embedded devices, disconnected networks, as well as the larger Internet.

(ii.) We need mechanisms to allow users to manage the privacy of their information, including information sensed about them by sensor networks or collected about their activities in cyberspace.

(iii.) We need mechanisms that allow us to balance privacy and accountability.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

(i.) The same test beds I mention above.

(ii.) We need enterprise-scale deployments of next-generation ICT environments to allow researchers to evaluate the usability and scalability of new mechanisms.

Eric Luiijf, TNO Defence, Security and Safety

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

(i.) Key challenges

- *Sticky/persistent security properties with the data,* e.g. content-based security (protecting the data elements all the times against confi and integrity threats)
- *Assurance of composite elements*

(ii.) Key technical issues

- Persistent security in SOAP
- Content-based security and information-sharing mechanisms
- Out-of-band QoS signaling across black-red divides (encryption; VPN)

(iii.) Environment

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

- Key challenges
- Key technical issues
- Environment

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

No comments

Discussion:

Grand Challenge(s) for S&D to reach breakthroughs?

Fabio Martinelli, National Research Council of Italy

Proviso: Before addressing specific research challenges for the EU-US cooperation as requested, I would like to stress the necessity of strengthening a long lasting cooperation between the two scientific communities.

Reinforcing EU-US cooperation from its roots: Formation!

There is an increasing demand of researchers working in research problems underpinning global security, and ICT security in particular. The European and North American scientific communities cooperate often together (at least at the individual researcher level). The two communities have slightly different and peculiar R&D methodologies and approaches. For establishing a long lasting and fruitful cooperation, exchange of ideas and results, and for maximizing the impact of this kind of research workshops, we could foster the creation of a global formation program for young researchers - Ph.D. students - (involving also industries). As a matter of fact, the lack of security and trust remains a main socio-technical obstacle to the fully development of information and knowledge society. We need to create *a new generation of computer scientists* that have a deep understanding of trust and security across all layers and the different technology paradigms as well as a strong awareness of the legal and business context within which future security and trust management solutions will operate. *This new generation of young scientists, exposed to the best research practices of both scientific communities, as well as of the corresponding industrial ones, will pave the way for a long lasting cooperation!*

We need to set up a critical mass of expertise and resources that is required in order to train such a new generation of researchers.

A first, practical step: An EU-US Ph.D. summer school on ICT security.

Currently, there are several research schools around the world that tackle ICT security. One with a long tradition is **the international school on Foundations of Security Analysis and Design (FOSAD)**, at its 7th edition since 2000. The school is under the auspices of the International Federation on Information Processing WG 1.7 on Security as well as of the Security and Trust Management WG of the European Consortium in Informatics and Mathematics **(ERCIM).** The school each year receives more than 80 requests for only 50 students. From US, there is a limited attendance, we feel mainly because of lack of travel funding.

The Steering Committee of the FOSAD School is EU-US based and the speakers come form both the communities, e.g., this is the list for 2007: *Ross Anderson, Ulfar Erlingsson, Cathy Meadows, Chris Mitchell, George Necula, Bart Preneel, Jean-Jacques Quisquater.*

Similar Schools exist in several forms also in the US. It would be interesting to create on top of these experiences a common EU-US liaison for fostering to a deeper level the cooperation between the two scientific communities.

A possible schema would be one School held in Europe and one held in US (yearly), where the money for travel and accommodation of the US young researchers to EU is paid by US, as well as the money for EU young researcher to travel to US is paid by EU. Other funding schemes may be implemented (e.g., EU pays US students for attending its School and vice-versa).

From EU side, a possible funding instrument could be Coordinated Actions as well as Specific Support Actions aimed at coordinating or supporting research activities and policies (networking, exchanges, coordination of funded projects, trans-national access to research infrastructures, studies, conferences, etc).

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability

Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

Holistic approach to trust management in service oriented architectures/infrastructures.

Integration of trust and reputation algorithms with security policy and negotiation strategies in order to allow an integration of trust management from both "strong and crisp" approach, where decisions are founded on logical rules and verifiable properties encoded in e.g., digital credentials, and a "soft" approach, based on reputation measures gathered and shared by a distributed community. In such an approach both verification methods based on rigorous design principles as well as probabilistic and social based notions of trust can be expressed, composed and analyzed.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

(i.) *Adaptive security and trust policy frameworks.* Policy languages and mechanisms should be developed for continuously managing security and trust levels in a system as well as contractual agreements in service oriented architectures. These policies should be able to adapt to the current context. Trust may be used in security related decisions (e.g., access and usage control) as well as it may be applied to ease privacy preserving policies (e.g., trust-based routing protocols). Policies may be also able to detect current attacks as well as to adapt the protection mechanisms. The capability to detect attack is also based on advanced and cooperative monitoring techniques.

(ii.) *Advanced real-time, collaborative and policy-based monitoring frameworks*. Both *proactive and reactive* monitoring techniques can be adopted. When a bad behaviour is detected, the information could be spread to other users in a reliable way. Behavioural policy languages would be useful for precisely expressing the allowed and the malicious behaviour (also incorporating some quantitative measures as probabilities an time). Also policy-based monitoring engines should be applied to appropriately monitor the entity behaviour from its "correct" specification as well as detecting and tracking malicious behaviours (attacks). This would be particularly useful on service oriented architectures where workflow engines elaborate languages for service provisioning. Collaborative monitoring approaches should be followed.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

(i.) *Benchmarks, validation and verification techniques and tools* for establishing the relative merits of each trust management framework. We need to define and implement a platform for trust management and reputation models assessment, comparison and validation. *Simulation* techniques, metric, *theoretical and analytical* comparison frameworks will be studied. Also selection and appropriate data to be mined will also another opportunity. A benchmarking framework should be open source and provide a reference implementation of the most well known trust and reputation models and metrics. In addition, it could provide standardised benchmarking data extracted from real online data, for example, by mining online social networks or open source repositories, to increase the applicability of the models and metrics in real applications. Anonymization procedures should be put in place when analyzing real data.

(ii.) *Possible cooperation mechanism:* Cooperation between existing/future research projects.

Roy Maxion, Carnegie Mellon University

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

Rigorous methods for experimentation and measurement.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

New language design that obviates the problems of today's vulnerability-prone languages (like C).

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

My answer to the previous section's (c) question would be about the same here.

Takashi Nanya, University of Tokyo

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

To secure the applications and services, a methodology are required to verify the trustworthiness of, and evaluate the dependability of, summarized and prioritized data from a huge amount of information produced and recorded on future polymorphic networked systems.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

At least two steps of approaches may be required. The first step should be to explore a new theory and technologies to handle an enormous amount of information produced and recorded on global networks everyday in the world to extract useful information for the society, business and international security. The second step should be to explore a methodology to verify the trustworthiness and evaluate the dependability of the summarized and most likely prioritized information.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

It is a question of vital importance for information societies to have test beds to verify and assure the dependability of information delivered by future polymorphic networked systems.

Vern Paxson, Lawrence Berkeley National Laboratory

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability

Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

I must say that the notion "future polymorphic networked systems" really is confusing to me - particularly, the term "polymorphic". Assuming it simply means "rich mix of different types of communications and communicating devices, then I think the key attributes remain those already well-recognized when considering system security: threat model + available resources + legal/policy constraints.

This is leavened with the consideration I sketched above regarding the degree to which communication semantics can be exposed/available to third parties; plus the difficulty that threat model will evolve over time, and thus cannot be designed for in advance.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

First, I don't know what CIP refers to. But even if I did, I don't believe mechanisms can be considered a priori. Rather, one must first understand the envelope imposed by legal / policy constraints, plus desired richness of the communication enabled by the network, plus available resources for meeting these.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

Same as above, though here even somewhat more vague, as I don't really know what "future polymorphic networked systems" are.

András Pataricza, Budapest University of Technology and Economics

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

I guess, IT has to learn from the safety critical area. Combined, standardized measures for the processes and products and services, like SIL in the SC area would be highly beneficial. On the other hand, the field of semantic webs lacks the characterization.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay /Infrastructure solutions, large and small scale security, long term security, middleware solutions?

The IT industry already offers a variety of solutions. Very little has been done by the academic community to help their introduction into the mainstream. Even in the case of the such traditional fields like system monitoring data integration into model based thinking in the analysis is still in its initial phase. Evolving adaptive and semantics based applications (like the semantic web) lack the well established and practically by using the academic background. Closed loop modelling is another field requiring more attention.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

I see as the first phase a distinguished importance to the integration of the existing modelling and formal analysis methods with the industrial practice, and a similar integration between the academic approaches addressing different aspects of dependability and security. In order to bring to such methodologies nearer to the end users, at least the academic community should address interoperability and integration of their tools.

Most probably a proper way would be the extension of existing industrial open standards by the aspects and attributes needed to model and analyze dependability and security. Tool integration could be done by means of a service based integration concept, but we successfully used in DECOS. The fusion of the approach is already existing in the academic world would have a huge synergetic effect.

Michel Riguidel, École Nationale Supérieure des Télécommunications

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

(i.) The first issue to be addressed is that of understanding trust in its multiple facets and manifestations: trust between people, between people and the cyber-infrastructure, among people using the cyber-infrastructure, in a society of human and software entities, finally in more complex value network and ecosystem settings. This should be a concerted multidisciplinary and truly international program.

(ii.) Based on this understanding, the next objective should be to engineer trust management and access control and policy systems. They should be flexible enough to understand and accommodate the dynamic nature of trust. They should integrate seamlessly with existing and future security systems, for example detection of fraud, intrusion attacks, other malicious behaviour, trust and risk assessments and relationship and access control policies.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay /Infrastructure solutions, large and small scale security, long term security, middleware solutions?

(i.) From Computer Science:

- Distributed systems and algorithms, security systems and technology, recommendation/reputation systems, access control technologies and systems, agent and personal assistant technologies,
- Standardization efforts in W3C, OMG, OASIS, GGF, etc.
- Formal and verification/certification methods and techniques, formal logic and modelling, fuzzy set theory to apprehend gradual trust and distrust, trust-related knowledge, and to tackle inconsistencies throughout trust recommendations.
- Mathematical and semantic models to measure, evaluate trust, cryptographic protocols, infrastructure, smart device and algorithms to collect data for trust, distrust, partial trust, partial knowledge, indirect trust, delegation of trust, graduation of trust, evolution of trust.
- Models of trust and security assurance evaluation of resources: a component (hardware, software), a set of components (networks, services), a constellation or a fleet of devices, very highly distributed components, graphs (semantic web).
- Models of trust with mobility (fast re-authentication), with discovery, with uncertainty or partial knowledge.
- Understanding of the dynamics of trust, on whether is can be inherited from people and systems by mutually trusting and trusted organizations, and of how systems based on trust

can remain flexible and handle possibly drastic change in, for example, value networks, and ecosystems.

(ii.) Appropriate branches of sociology (for example mathematical sociology, social and exchange networks, etc.), psychology, ethics, legal studies (particularly informatics and law), economics and game theory.

- Promotion of a multi-disciplinary framework for the analysis of the performance of trust mechanisms.
- Consideration of the socio-economics of trust in the modelling of complex systems.
- Theories and methods for assessing the impact of levels of trust on the deployment, economic viability and social acceptance of systems and services.
- Socio-economic implications of threats: extended risk management, crisis management models to minimize damages of unexpected events.
- Support of human beings (end users and not only experts) being adequately in the control loop to enforce a trust behaviour.
- Usability of security procedures and tools.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

(i.) One of the biggest inhibitors of growth of use of the Internet for human interactions (commercial or otherwise) has been the lack of trust in the underlying cyber-infrastructure and in other people whom we meet through that infrastructure. This not only affects B2C transactions, it also generates hesitation in companies or virtual communities in general, to engage in tight, seamless, transparent relationships among each other, thus forming networks - which are usually called virtual organizations (VOs) or value networks. Recent incidents of massive identity theft from financial institutions that are otherwise internationally respected for their trustworthiness, and the never-ending resourcefulness of malicious hackers and intruders have increased the apprehension and uneasiness of the general public vis-à-vis the Internet and Web use.

(ii.) The grand challenge is the reversal of this climate on a global, planetary scale, not only at the level of interactions among human agents (commercial or otherwise) through use of the cyber-infrastructure, but also among human and software agents, and any arbitrary groupings thereof. These groupings may form hierarchies of value networks, business and/or cultural ecosystems, industry segments, social networks, whole societies or nations etc.

(iii.) Trust is a concept that is broadly shared by mankind. One can objectively think that human beings would have trouble facing the complexity of this world without relying on trust, as they base themselves on that notion to assess the various options they have in everyday life. Some define trust as entrusting one's fate to somebody else and betting the latter's action will have a positive outcome. Others consider this definition to be loose, as it does not specify clearly that the risk incurred by entrusting one's fate to somebody else must be small compared to the potential benefit one could draw in the event of a positive outcome. Some however, consider the latter definition to be too stiff, as they find it excessive to entrust one's fate to somebody else without being able, at one time or another, to influence the latter's actions. Although myriads of works of sociology, psychology, philosophy, and anthropology, have been devoted to trust, it is difficult to delineate that concept. Partial trust, partial distrust to share information, and reputation or recommendation systems continue to challenge our conceptions.

(iv.) How trust emerges and vanishes among people or among groupings of people (institutions, communities, etc.), until recently without use of a cyber-infrastructure, is an open, multifaceted and interdisciplinary problem. What is needed is an understanding of the trade-offs between trust and

privacy, trust and security, as well as trust between commercial possibly competing partners and the safekeeping of proprietary strategic differentiating assets.

(v.) Any understanding reached from the previous questions, should be mapped on the problem of understanding, engineering and managing trust from people to the cyber-infrastructure. The cyber-infrastructure should be used to generate and manage trust among people in non-traditional ways and in a global planetary scale (for example among people who live far apart, have never seen each other, do not know of each other, but who however see benefit, commercial or otherwise, in a cyber-infrastructure enabled interaction). It should also be extended to societies of human and software agents and to arbitrary interacting complex network structures thereof.

Reijo Savola, VTT Technical Research Centre of Finland

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

(i.) Prioritized technical issues to address over the next 3 years:

1. Trustworthiness of services, networks and devices
2. Privacy of user data
3. Usability of security, trust and dependability solutions

(ii.) Suggested mechanisms to establish EU-US co-operation:

- Aggregation of state-of-the-art knowledge
- Co-funded research projects with case examples from industry (both EU and US)

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

(i.) Prioritized technical issues to address over the next 3 years:

1. Automated security level estimation mechanisms based on context and history information
2. Smart intrusion prevention & detection: Aggregation of measured information using smart algorithms
3. New Internet paradigm

(ii.) Suggested mechanisms to establish EU-US co-operation:

- Aggregation of state-of-the-art knowledge
- Co-funded research projects with case examples from industry (both EU and US)

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

(i.) Prioritized technical issues to address over the next 3 years:

1. Security, trust and dependability metrics models
2. Monitoring systems for security
3. Testing systems

(ii.) Suggested mechanisms to establish EU-US co-operation:

- Aggregation of state-of-the-art knowledge
- Co-funded research projects with case examples from industry (both EU and US)

Jason Smith, Queensland University of Technology

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

(i.) Identity is an important conceptual attribute in emerging MMEs. More particularly, layer appropriate concepts of identity will be required if there is to be any expectation that meaningful tradeoffs between security and privacy are to be made. Determining the requirement for identity at the application, network and device layers is not yet fully understood, or specified, and the identity of individuals can be used inappropriately.

(ii.) Other key attributes include the trustworthiness of devices (both hardware and software), assurance of compliant behaviours or the ability to assess (and possibly enforce) compliant behaviours.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

(i.) Where trust in the hardware and software used by devices in a highly interconnected MME cannot be assured, mechanisms that permit the monitoring and evaluation of behaviour of such devices must be possible to ensure that these behaviours conform to expectations.

(ii.) One specific area where this is a requirement already is the area of compliant cryptologic protocols. In compliant cryptologic protocols, two mutually mistrusting entities are able to ensure that the protocol they engage in conforms to specific requirements, requiring them only to trust in the design of the security system, not the other entity. In this way compliant cryptologic protocols act as a broker between the mistrusting entities.

(iii.) Balancing the need for lightweight devices to leverage sufficient security (constrained by their computational and storage resources) and the provision of supporting infrastructure of a scale suitable for use in networks orders of magnitude larger than current networks is challenging.

(iv.) While the use of virtualisation to address current problems is intuitively appealing, significant issues of trust, when virtualised instances of processes migrate between platforms for example, remain to be addressed.

(v.) The traceability of actions, in an environment where services are dynamically composed, and the preservation / accessibility of forensic evidence in polymorphic networks and MMEs will be far more difficult. Identifying the correct balance between security and privacy concerns of evermore pervasive systems remains an open problem.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

Fundamental problems in provable security suggest that current formal models of (cryptographic) security are unlikely to be able to deal with the complexity associated with analysing the protocols adopted by large scale MMEs, unless advances are made in the composability and reusability of proofs.

Neeraj Suri, Technische Universität Darmstadt

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

Need to figure out the (a) the interplay across S & D, and (b) a service-model outlook prior to meaningfully scoping the problem. What are the S&D policies?

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

I would rather worry about first defining the core MME policies (see Theme 1 (a-b)) prior to the mechanisms.

Wade Trappe, Rutgers University

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

(i.) *Cross-layer information:* It is increasingly unlikely that layered security mechanisms will be sufficient to address security threats. The next generation of security mechanisms will need to exploit information gathered across multiple network layers. For example, physical layer information is being identified as a critical layer for localizing wireless transmitters. More hooks into lower layers of the protocol stack are needed so as to extract this information.

(2) *Non-mutable device identities:* One of the problems with the current communication infrastructure is that device identities can be changed (e.g. using ifconfig to change MAC addresses in WiFi networks leads to device spoofing). This problem makes it hard to hold devices accountable. Some form identity that is inserted at the hardware in a tamper-proof manner, would greatly support auditing, blacklisting, etc.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

(i.) Cross-layer security protocols: Protocols that take advantage of information across multiple layers will be able to exploit these multiple layers of information to make more accurate assessment of network intrusions, etc.

(ii.) Location Security: Location information, if verifiable, can provide a means to discriminate between entities, allow for new security policies (e.g. you may only access a file if in a certain location), etc. In particular, it adds an extra dimensionality to our ability to protect networks.

(iii.) Trusted platforms and tamperproof memory: We need platforms with the ability to run reference-monitoring on processes at fine time granularity. As many technologies move increasingly towards open-source development, we will have a challenge to ensure that the software running on these platforms are fair or non-malicious (e.g. a device that is utilizes a greedy TCP protocol). As an example, software defined radios represent a dangerous attack platform with highly programmable access to lower layers.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

(i.) Software Defined Radio/Cognitive Simulator and Test bed: One domain that I am particularly concerned about is the security of software radios (or, their newer form, cognitive radios). This platform allows for arbitrary access to the lower layers of the protocol stack, and can be easily used for a variety of attacks, from jamming to being able to serve as a protocol-mutable rogue access point. Although there are several efforts to develop these platforms, and the security work is quite limited, in large part due to the fact that the technology is still quite immature. We need to build models for the operation of these platforms now (before the problem gets out of hand), create simulators for the operation of these cognitive radios so that we can devise security mechanisms, and then be prepared to develop and evaluate these solutions as cognitive radio platforms become available.

(ii.) EU-US Mechanisms for Co-Operation: The EU-US should encourage researchers to consider the problem of security in systems that are highly-programmable (such as software radios). We tend to not think about the level of programmability that our current networked-PC world has (frankly, its not too programmable when you consider the fact that many functions are firmware/hardware restricted). There is an abundance of research problems in the domains of highly-programmable devices, ranging from defining security policies to fast-verification of policy compliance to software attestation.

Alfonso Valdes, SRI International

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

As with theme 1, security across interfaces and composable security are key. We should advance further opportunities for fault and attack tolerance (example in the CIP case, graceful degradation to disengage from public networks and then operate with local knowledge and only limited global awareness (also speaks to "adaptation" in (b)). How do we stand up trusted ad hoc communications (for example, in cross-border crisis response)? We must ensure reliability and robustness as complexity increases (positive example from modern aircraft, which are simultaneously more complex yet safer than past designs).

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

For all these solutions, usability is the big barrier. Particularly in CIP (if I understand how it is meant here), many of these solutions are difficult to implement for technical and cultural reasons. Users should have trusted (in the CS sense as well as the colloquial sense) mechanisms to authenticate only to the degree necessary for a particular transaction.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

Usability demonstrations are key to any proposed solutions. CIP test beds, data sets, and models must comprehend real time issues in, for example, power distribution, which has cross-border aspects. Implementing faithful models of international financial markets poses a formidable challenge.

Aad van Moorsel, University of Newcastle

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

(i.) A first element to realize in modern-day, Internet-based, multi-mode systems is that dependability requirements do no longer allow themselves to be captured or specified a priori as requirements. Instead, changing environments will continuously require one to adjust the dependability needs and emerging system behaviour will keep surprise engineers with unforeseen security breaches, threats and attacks. Taking this to its logical conclusion, the traditional scientific approach to define a property, divine an abstraction and then provide an algorithm to provide the property assuming the abstraction will no longer work. Instead, continuous monitoring, tinkering and tailoring is necessary, and the challenge therefore lies in executing this (by its nature ad hoc) process reasonably systematically.

(ii.) Neither security nor trust comes with a natural metric to establish its fulfilment. As opposed to QoS (response time, loss probability, throughput) or, to a large extend, reliability (mean time to failure, down time), we do not know how to quantify the difference between the security or trust of two alternative designs. Arguably, QoS metrics are the ones that count, and security should ideally be evaluated with respect to its impact on QoS, but in reality we do not know how security impacts QoS and metrics that allow us to trade off, for instance, encryption technologies in various situations are necessary.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

As a consequence of above, systems need to be adaptive to the circumstances in which they end up operating and being used. Automation of dependability provisions need to be balanced by the ability of the human to interfere or take over decision-making when decisions by nature are subjective and require hard to encode judgements and trade-offs. Without good techniques, methodology and best practices, security engineering trivializes to binary argumentation about ‘secure’ or ‘non-secure’ systems.

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

Excerpt from “Public Repositories for Failure Data: Technologies and Policies”, by Bojan Cukic, Dan Dobre, Myron Hecht, Andreas Leitner, Brendan Murphy, Bianca Schroeder, Carol Smidts, Neeraj Suri, Aad van Moorsel (Ed.), Reliability Analysis of System Failure Data workshop, Microsoft, Cambridge, 2007:

Vision: diagnosis and quantitative assessment of real-world software and systems requires data, but data collection is often a time-intensive task for researchers and engineers. To facilitate reuse of data, public data repositories are necessary.

To enable the vision of a public data repository, we suggest the following steps:

1. establish a universally accepted definition of the content of a failure data set, in order to establish trust in and widespread acceptance of analysis results
2. initiate grass roots efforts to set up data repositories

3. create ‘open dump’, a central but open, independent place for storing failure data
4. create an industry consortium that advocates and enables sharing of quality data

We furthermore observe that a data repository dedicated to operating system failure data may be particularly appropriate, because of the richness and well-understood, stable nature of the data involved. Operating system failure data may therefore be a good first candidate for which to implement our suggestions.

Excerpt from contribution to 2006 EU/US workshop on Cybertrust in Dublin:

Service-oriented software and utility-computing inspired service provisioning systems are being developed in many places. Realistically, the complexity and scale of such systems makes it difficult for academia and small/medium businesses to effectively try out their ideas. A test bed that allows realistic experiments to be run would open up opportunities for these parties to venture into service-oriented solutions.

Existing world-wide test beds Planetlab and GENI (Global Environment for Network Innovation), target, as the name explicitly indicates in the second case, network innovation. These platforms allow for almost unrestricted experimentation, but necessitates every user to install application level software from scratch. Reuse of application level solutions is difficult.

The envisaged test bed would allow for experiments such as the following:

- experimentation with security policies for computing service providers
- experimentation with bandwidth and computing reservation algorithms in fully virtualised environments (as in Violin)
- experimentation with fault tolerance solutions such as mediators using realistic web services
- experimentation with new services deployment solutions on top of virtualised environments (services as in GOLD and other projects)

The kind of technologies we envision being provided by a software and services test bed are, among others:

- virtual machines (such as Xen), virtual distributed environments (as for instance proposed in Violin)
- realistic Internet services (B2B services, medical applications, bioinformatics services, etc.), using various technologies (web services, REST)
- load balancers, firewalls, and other parts of realistic service provisioning systems
- service deployment software (as for instance in DynaSOAR or Smartfrog.org)

Jody Westby, Global Cyber Risk LLC

(a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

It is imperative that a dialogue begin between the US-EU and Asia regarding the harmonization of privacy laws, data retention, and security breach notification. Until such time that there is a harmonized framework, the technical solutions will continue to run into trust quagmires.

(b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP/Overlay/infrastructure solutions, large and small scale security, long term security, middleware solutions?

Legal and policy issues must be factored into the development of mechanisms so they are not purely technical in approach, but take into account the cultural, legal, and operational aspects of all systems. S&D are cultural concepts that are extended into the law. These cultural and legal considerations must be factored into the development of monitoring schema, crypto, CIP/Overlay/infrastructure solutions, and security and middleware solutions.

(c) What sort of test beds, datasets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

The DHS PREDICT project and its approach to developing a test network and test datasets comprised of real traffic data offers a valuable example to R&D teams, government officials, policymakers, and industry.

Appendix C – Final Agenda

Molly, please put final agenda here. I cannot find a Word version of this.

Appendix D - Workshop Participant List

Tom Anderson
University of Washington
UW Mailbox 352350
Seattle WA 98195
USA
phone: 206-543-9348
tom@cs.washington.edu

Michael Bailey
University of Michigan
2260 Hayward Avenue
4611 CSE, University of Michigan
Ann Arbor MI 48109
USA
phone: 734-647-8086
mibailey@eecs.umich.edu

Roberto Baldoni
Università di Roma "La Sapienza"
Via Salaria 113
Roma 198
Italy
phone: 3.9064991848e+011
baldoni@dis.uniroma1.it

Paul Barford
University of Wisconsin
1210 West Dayton Street
Madison WI 53706
USA
phone: 608-262-6609
pb@cs.wisc.edu

Robin Bloomfield
Centre for Software Reliability
City University
Northampton Square
London EC1V 0HB
United Kingdom
phone: +44 (0)20 7040 8896
reb@soi.city.ac.uk

Sandro Bologna
ENEA
Via Anguillarse, 301
Rome 123
Italy
phone: -30483675
bologna@casaccia.enea.it

Nikita Borisov
University of Illinois
460 Coordinated Science Lab
1308 West Main Street
Urbana, IL 61801
USA
phone: 217-244-5385
nikitab@gmail.com

Jacques Bus
European Commission
Office BU25 3/131
Brussels B-1049
Belgium
phone: +32 2 296 81 16
jacques.bus@ec.europa.eu

James Clarke
Waterford Institute of Technology
Cork Rd
Waterford
Ireland
phone: 35371916-6628
jclarke@tssg.org

Marc Dacier
Institut EURECOM
2229 Route des Cretes
BP 193
Sophia Antipolis 6904
France
phone: +33 4 93 00 81 64
secretariat@eurecom.fr

Helen Gill
The National Science Foundation
4201 Wilson Blvd
Arlington, VA 22230
USA
phone: 703-292-5111
hgill@nsf.gov

Elsa Gunter
University of Illinois
1332 Siebel Center
201 North Goodwin Ave
Urbana, IL 61801
USA
phone: 217-265-6118
egunter@uiuc.edu

Carl Gunter
University of Illinois
4304 Siebel Center
201 North Goodwin Ave
Urbana, IL 61801
USA
cgunter@uiuc.edu

Pieter Hartel
University of Twente
P.O. Box 217
Enschede 7500 AE
Netherlands
phone: 31534892411
pieter.hartel@utwente.nl

Ravi Iyer
University of Illinois
202 Coordinated Science Lab
1308 West Main Street
Urbana IL 61801
USA
phone: 217-333-2510
iyer@uiuc.edu; jlreese@uiuc.edu

Richard Kemmerer
UCSB
University of California
Santa Barbara CA 93106
USA
phone: 805-893-4232
kemm@cs.ucsb.edu

George Kesidis
Penn State
338J IST Building, CSE Dept
University Park PA 16802
USA
phone: 814-865-9190
kesidis@engr.psu.edu

David Kotz
ISTS--Dartmouth College
45 Lyme Road, Suite 300
Hanover NH 3755
USA
phone: 603-646-0717
dfk@cs.dartmouth.edu

Karl Levitt
The National Science Foundation
4201 Wilson Blvd
Arlington, VA 22230
USA
phone: 703-292-5111
klevitt@nsf.gov

Eric Luiijf
TNO Defence, Security and Safety
P.O. Box 96864
The Hague ZH 2509 JG
Netherlands
phone: +31 70 3740312
eric.luiijf@tno.nl

Fabio Martinelli
National Research Council of Italy
Via G. Moruzzi 1
Pisa I56100
Italy
phone: 3.9050315343e+011
Fabio.Martinelli@iit.cnr.it

Douglas Maughan
U.S. Department of Homeland Security
Washington, D.C. 20528
USA
phone: 202-282-8000
Douglas.Maughan@dhs.gov

Roy Maxion
Carnegie Mellon University
5000 Forbes Ave
Pittsburgh PA 15213
USA
phone: 412-268-5576
maxion@cs.cmu.edu

John McHugh
Dalhousie University
Faculty of Computer Science
6050 University Ave.
Halifax NS B3H1W5
Canada
phone: +1 902 494 3048
mchugh@cs.dal.ca

Klara Nahrstedt
University of Illinois
3104 Siebel Center
201 North Goodwin Ave
Urbana, IL 61801
USA
phone: 217-244-6624
klara@uiuc.edu

Takashi Nanya
University of Tokyo
4-6-1, Komaba, Meguro-ku
Tokyo 153-8904
Japan
phone: +81 3 5452 5160
nanya@hal.rcast.u-tokyo.ac.jp

David Nicol
University of Illinois
457 Coordinated Science Lab
1308 West Main Street
Urbana IL 61820
USA
phone: 217-244-1925
nicol@iti.uiuc.edu

András Pataricza
Budapest University of Technology and Economics
Department of Measurement and Information Systems
Magyar tudósok krt 2.
Budapest H-1117
Hungary
phone: +36 1 4633595
pataric@mit.bme.hu

Vern Paxson
ICSI / LBNL
1947 Center St. Suite 600
Berkeley CA 94704
USA
phone: +1 510-666-2882
vern@icir.org

Michael Reiter
Carnegie Mellon University
5000 Forbes Ave.
Pittsburgh PA 15213
USA
phone: 412-268-1318
reiter@cmu.edu

Michel Riguidel
ENST
46, rue Barrault
Paris 75013
France
phone: 33 1 45 81 73 02
riguidel@enst.fr

William Sanders
University of Illinois
451 Coordinated Science Lab
1308 West Main Street
Urbana, IL 61801
USA
phone: 217-333-0345
whs@iti.uiuc.edu

Reijo Savola
VTT Technical Research Centre of Finland
Kaitovayla 1
Oulu - 90570
Finland
phone: +358 20 722 2138
Reijo.Savola@vtt.fi

O. Sami Saydjari
Cyber Defense Agency, LLC
3601 43rd Street South
Wisconsin Rapids WI 54494
USA
phone: 715-424-2642
admin@cyberdefenseagency.com

Jason Smith
Queensland University of Technology
Information Security Institute
126 Margaret Street
Brisbane Queensland 4000
AUSTRALIA
phone: +61 (7) 3138-9570
j.smith@isi.qut.edu.au

Neeraj Suri
TU Darmstadt
Dept. of Computer Science
TU Darmstadt
Darmstadt HE 64289
Germany
phone: (011) 49 1609065 9435
suri@informatik.tu-darmstadt.de

Wade Trappe
Rutgers University
671 Rt. 1 South
North Brunswick NJ 8902
USA
phone: 732-932-6857
trappe@winlab.rutgers.edu

Alfonso Valdes
SRI International
333 Ravenswood Ave
Menlo Park CA 94025
USA
phone: 650.859.4976
alfonso.valdes@sri.com

Aad VanMoorsel
University of Newcastle
Newcastle
UK
phone: 3.2421321321e+011
aad.vanmoorsel@newcastle.ac.uk

Jody Westby
Global Cyber Risk LLC
4501 Foxhall Crescents NW
Washington DC 20007
USA
phone: 202-337-0097
westby@globalcyberrisk.com

Appendix E – Criteria for International Collaborative Research on Security and dependability

To be appropriate for the intended programme of international collaborative research between EU and US on Security and Dependability, potential research projects **should be of common interest and fit one or more of the following criteria**:

International Scale: topics relating specifically to systems that are inherently international in character and which are challenging enough and necessary to merit being tackled on an international scale (e.g. through the global scale of problems to be addressed)

Complementarity: topics for which there is useful complementarity of expertise or resources, beyond what is readily available without collaboration (e.g. topics that involve highly complex ICT networks and systems, or which make use of a variety of pre-existing or launching new test-beds)

Cultural Differences: topics raising different aspects between the countries and cultures involved in the collaboration (e.g. ones related to personal data protection, or to differing national attitudes to trust)

Additional Issues: topics which address issues that arise from or are greatly affected by the co-existence of disparate, and potentially incompatible, legal regimes (e.g. concerning cyber-crime)

An initial list of priority areas concerning the planned EU/US collaboration on Security and Dependability research were identified at the Dublin workshop in November 2006. These are topics that the officials from both sides regarded as fitting their organisations' plans and policies, and which the representatives of the two research communities felt were timely, significant, and technically challenging, while complying with the above selection criteria.

One may expect that at the Illinois workshop in April 2007, this list of priority areas will be refined or augmented. We, therefore, challenge all invitees, and invited speakers in particular, of the Illinois workshop to:

(i) identify and describe particular projects and areas of interest to them that fit both the criteria and our current priority areas, and

(ii) provide a justification for their choice.

However, invitees are also invited, should they so choose, to suggest and provide arguments for possible improvements both to the list of criteria, and to the list of priority areas.