Main conclusions of the EU-US Summit on "Cyber Trust: System Dependability & Security", held in Dublin 15-16 November 2006

The workshop of the EU/US Summit Series on "Cyber Trust: System Dependability & Security" was held in Dublin, Ireland on November 15th and 16th, 2006. It was attended by 60 delegates from the EU and the US, along with representatives from Canada, Australia and Japan. This event was co-organised and hosted by Waterford Institute of Technology (WIT), the project co-ordinator of the IST-FP6 Co-ordination Action SecurIST, and also co-organised by the US National Science Foundation (NSF), Department of Homeland Security (DHS), University of Illinois, and the European Commission, Directorate General Information Society and Media, Unit D4 "ICT for Trust and Security".

The aim of this workshop, and a planned follow-up workshop to be held in Illinois in April/May 2007, was to gain a shared understanding of critical issues, identifying promising dependability and security research directions, and also to foster collaboration between EU and US research teams.

The organising committee of the workshop developed the programme around the following themes within Trust, Security and Dependability (TSD) of future networked systems: Architecture and design issues, scalability and context awareness, security and privacy in dynamic wireless networks, TSD predictive evaluation and assessment approaches and future test-beds.

The workshop discussions led to identification of a number of research challenges, scoping research priorities and joint actions to address them.

Cyber Trust Summit in Dublin, Organising Committee. From left to right: Michel Riguidel (ENST), David Du (NSF), Jacques Bus (EC), Thomas Skordas (EC), Karl Levitt (NSF), William Donnelly (Waterford IT), William Sanders (U. of Illinois) and Brian Randell (U. of Newcastle).

The main workshop themes and their conclusions are presented below. The list of participants and all presentations and position papers are available on www.securitytaskforce.eu. A workshop report will be published by the end of January 2007 and will be available on this website.

The workshop themes and their conclusions

(1) ***Architecture and design issues for TSD of Future Networked Systems*** Topics discussed under this theme included new TSD attributes, protocols, adaptive detection, diagnosis, and run-time response mechanisms and stochastic security in core/access networks from an end-to-end perspective.

Future emerging networked systems will likely be mixed mode environments consisting of diverse computing, communication & storage capacities and will be based on the model of service-centric computing. For these new environments, there is a need to specify not only the underlying service semantics but also the TSD semantics and metrics for designing resilient architectures and secure network protocols and for detecting and measuring any anomalous behaviour.

Regarding the design for resilience, we need to reconcile the predictability desired of systems with the uncertainty we get from the environment. We need to design network infrastructures that are resilient to some routers acting maliciously and distributed information systems that are resilient to some servers being compromised. There is a requirement in particular for new paradigms on Internet routing as routing security involves several complex issues where solutions are not yet identified. For example, we need to design for route discovery based on social keywords and their potential aggregation, with separation of identity and *routability*.

We need also to secure the underlying poly-infrastructures composed of many heterogeneous networks and devices; to build distributed crypto in large scale networked systems by distributing critical operations and refreshing secrets shared between multiple nodes without a single long-term secret being present in one node; to deal with small-scale security, i.e., securing devices that have scarce resources by protecting interfaces through ultra low-power and low-footprint crypto and by sharing security among joints; to secure dynamic virtual entities spanning from persons to organisations and to whole nations; and, to develop security for long term data storage and archiving (50-100 years) and thereby to design cryptographic algorithms and their secure implementation.

For these mixed mode environments, security-by-design is desirable if achievable. There is an additional need though to develop *adaptive, negotiable, end-to-end run-time TSD enhancers* and provide an end-to-end specification of the operational environment for the duration of the desired services to a specified level of trustworthiness. Automated fault detection and remediation on a massive scale is required, along with application-aware detection of malfunctions and software vulnerabilities and application-specific reconfigurable and scalable trusted computing platforms.

(2) ***Scalability and context-awareness for TSD of Future Networked Systems*** In this theme, discussions focused on multi-layered, scalable and context-aware approaches to make networked systems secure and dependable. The main conclusions being:

Current systems are often built from commodity unreliable hardware and software. From the hardware perspective, scaling is associated with VLSI/processor level reduction in hardware line widths, increasing device densities, the subsequent increasing design defects as well as with building approaches to software containment. From the software and system perspective, we need to extend scalability through better, realistic abstractions and by focusing on three phases of the lifecycle: (a) Requirements capture – incl. citizens, (b) System design, and (c) Evaluation and testing.

We need systems-level analysis and confidence through proof based techniques at that level. We need to develop a formal authorization engineering framework, as the lack of authorization capability limits the scope of systems that can be considered.

We need to move towards autonomic system-of-systems health management approaches that enable automated fault detection and remediation on a massive scale. This includes, for example, the development of scaling approaches for network intrusion detection and response by exploiting parallelism, i.e. by implementing scaleable parallel intrusion detection methods.

In the internet driven computing world, the network or computing boundaries are no longer clear and anyone can set up a network; we, therefore, need to build intelligence into networks so that they can recognise rogue elements. In this context, we need security to include all levels, infrastructure, applications, services and human processes, and citizen empowerment i.e. giving the citizen the control and awareness of TSD to enable trust and guarantee privacy and confidentiality.

(3) ***Security and privacy in dynamic wireless networks*** of evolving systems composed of *ad hoc* coalitions of large numbers of sensors and devices for new personalized services. The main conclusions of the discussions held under this theme are as follows:

Dynamic wireless networks face many problems today. There is a lack of a security infrastructure, of threat models and of adequate security evaluation techniques. There is an evident risk of loss of privacy when using such networks. Systems need to effectively perform basic operations (e.g., routing, membership) in adaptive contexts. There is also a need to consider risk management approaches as well as to address the control, configuration, and usage of ubiquitous devices.

It was suggested to "break out of the loop" of small problems and partial models. The main issues to tackle concern the protection of sensitive information, the network topology, the biometric information, the identity, and, the ability to manage the risk associated with their loss. The core challenge here is about the creation of secure, cost effective and usable systems. The main research directions agreed to address this challenge were the following: Testing methods and threat models; security infrastructure akin to tethered networks; adaptive systems based on context; trust management while giving users more control over choosing risk levels and adaptable context; and, usability of security systems, especially in complex heterogeneous sensor systems.

(4) ***Modelling, simulation, predictive evaluation, assurance cases for evaluating the TSD of networked systems*** The main issues addressed under this theme were verification and evaluation frameworks related to (possibly) Internet-scale applications and to particular networks and networked systems. The main points made are as follows:

For evaluating the TSD of networked systems, we need to consider the wider socio-technical aspects and interdependencies as well as their semantic learning and understanding dimensions. It is useful to adopt economic theory & security valuation that can assist multi-objective trade-off decisions.

There is also a need to use assurance cases and claim semantics from and for different stakeholders' viewpoints in order to communicate assumptions and agree on system security. Scenario building and use case generation may be valuable in this regard. In particular, there is a need to involve industry, governments and end-users for determining accurate, quantifiable TSD metrics and models. Subjective assumptions, reasoning and evidence need to be made explicit and visible as part of a probabilistic approach. Models need to quantify and analyse the business case and adversary attacks probability. Additionally, to be useful, metrics and measurements are required to be very detailed and specific.

Related research priorities that were highlighted include: Develop methods to deal with the intelligent and innovative attacker: in particular, how to deal with the unknown and perhaps even the "unknowable unknown". Investigate mechanisms to incorporate the different valuation systems of different stakeholders including both normal players and a range of adversaries, as well as methods to build trustworthiness and metrics into vendor products. Devise metrics to make intelligent engineering decisions based on probabilistic and Bayesian analysis. There is a need here to develop and use standard metrics for incremental security improvements and probabilistic approaches for radical security improvements and for reducing stakeholders' interdependencies.

(5) ***Monitoring, operational assessment, auditing for evaluating the TSD of Networked Systems*** Discussions focused on dynamic, online, analysis and evaluation methods and on real time assessment

frameworks, including attacks observed, observation mechanisms, audits, measurement and decision making tools, etc.

The main research challenges identified were as follows: Exhortation with respect to metrics, measurements, analysis: it is imperative to start now, with limited systems and goals, to gain basic understanding. Many particular problems are induced by the inherent dynamicism of systems, users and threats. There is need for threat characterization, prediction and observation. Instrumentation and data collection play a key role for diagnosis, whether manual or automatic. There is a need to use on-line measurements to control and adapt, in particular, to put in place network information sharing techniques at all levels (including attacks observed, keystrokes of users, network traffic capture in an anonymous fashion and others). Headway is being made in the legal framework but there is lack of incentives for providing and sharing data. While there is need to have more data, it is also indispensable to ensure sufficient context that would permit replication through experiments.

(6) Establishment of ***interconnected and/or common test-beds*** Discussions held under this theme addressed the opportunity for interconnecting existing experimental facilities and building joint benchmarks, test scenarios and interconnected test-beds for supporting the testing and evaluation of new dependability and security architectures, technologies, protocols, privacy protection mechanisms, etc., together with support towards global standards.

It was felt that this could lead to a significant increase in the extent and effectiveness of transatlantic co-operation in this research domain. One area of potential collaboration was of test-beds for networked systems. The need for developing a predictive science for networks was expressed. The issue is not only about having methodologies for comparative assessments, but actual test-beds (including simulation/emulation) that could help with the assessment. We could use a "data warehousing" approach to analyse, cross-exploit and share test-bed results. To further leverage this collaboration, knowledge collection and management mechanisms need to be established. In doing these, we need to find the right balance between details and rigor versus speed and inaccurate results and between generalisation versus specificity and the utility of the results.

Another area of potential collaboration discussed was a future shared test-bed for software and services to allow experimentation at the application and services level. Such a facility would enable other classifications of users, who ordinarily find it very difficult or even impossible to set up their own application and service provisioning environments, e.g., Academia and SMEs, to effectively try out their ideas in these environments without the overhead, time, expense and skill base required in setting up the required underlying infrastructure from scratch. Therefore, a test-bed of this kind that allows realistic experimentation would open up valuable opportunities for these parties to venture into service-oriented solutions. It would also allow consideration of the business issues of fair markets and to ensure the balance of privacy and accountability.