

## **PAMPAS Workshop**

16-17<sup>th</sup> September, Royal Holloway College, University of London, Egham.

### **Position paper**

P Y A Ryan, University of Newcastle

A number of initiatives in the area of dependability, security and privacy have been established as additional measures under Framework 5 or as Expressions of Interest for Framework 6. We briefly outline a number that are relevant to PAMPAS (and in which Newcastle has an involvement):

- AMSD/ISDI, FP5 accompanying measure/FP6 IP
- RAPID, FP5 accompanying measure.
- ESORICS NoE, a FP6 Expression of Interest in Establishing a Network of Excellence.

### **Background**

Complex, critical information systems will be ever more prevalent in all facets of society in Europe in the 21<sup>st</sup> century. Information technology has enormous potential to help realise the social and economic ambitions of the Community. At the same time, this technology and the increased reliance on it introduces new and greater risks. If this potential is to be realized we must ensure that the technology and infrastructure that is deployed is dependable. (Here we take the term dependability to cover such requirements as reliability, availability, security and privacy.)

Various recent EU publications have, either implicitly or explicitly, testified to the need for much higher, and more cost-effective levels of system dependability than is typically achieved by many of today's complex ICT systems. For example, the Presidency Conclusions of the Lisbon European Council (23 and 24 March 2000) and the action plan for eEurope envisage a Europe which by 2010 will be making widespread use of computer systems for many highly demanding and complex tasks. These documents stress the need for the information infrastructure, and the systems dependent on this infrastructure, to be adequately secure (and, more generally, dependable), and to be worthy of the high levels of trust and confidence that governments and citizens will have to place in them.

It is clear that the requirements of dependability, security and privacy are closely related. In particular, the requirements to secure infrastructures against criminal or terrorist acts can create "counter-threats" to civil liberties and privacy. It should also be stressed that many of the problems and solutions are socio-technical rather than purely technical. Consequently a unified approach to addressing these challenges and seeking to balance the requirements of the various stakeholders is essential.

### **AMSD/ISDI**

The AMSD FP5 Additional Measure is undertaking (i) a road-mapping exercise on Dependable Embedded Systems in preparation for FP6, alongside the other road-mapping exercises and initiatives on particular facets of dependability that various other groups are undertaking, and (ii) an exploration, of whether and how all the dependability-related activities in FP6 might form part of a coordinated overall programme. (This latter is in response to the fact that the form of the new instruments under FP6 is as yet not entirely clear. The scale, nature and inter-relationship of the new projects in the area of dependability, security and privacy are therefore not yet determined.)

The term that AMSD is using for such a coordinated overall dependability programme is ISDI (Information Societies Dependability Initiative). This is envisaged as encompassing a full range of dependability-related activities, e.g. industrial and long-term RTD on the various aspects of dependability per se, (reliability, safety, security, survivability, etc.); education and training; and means for encouraging and enabling sector-specific IST RTD projects to use dependability best

practice. In preparation for such an Initiative, AMSD has established a very broad membership, and is conducting what might be termed a meta-road-mapping activity, aimed at synthesizing and integrating the various more specific road maps that are currently being developed by various groups.

There is continuing evidence of considerable support in Brussels for such an Information Societies Dependability Initiative, which present thinking indicates could encompass multiple IPs, NoEs, and Targeted Projects, and be coordinated either from within the IST Directorate, or via some external organization set up for the purpose. Indeed, subsequent to the approval of the AMSD Proposal, an invitation was received to prepare an EoI based closely on the plans the Proposal contained regarding ISDI.

Further information about AMSD, and ISDI, is to be found at [www.am-sd.org](http://www.am-sd.org).

## **RAPID**

RAPID aims at developing a strategic roadmap for applied research in the area of 'privacy and identity management'. The project will build a robust platform of leading experts and stakeholders and provide a forum to develop a detailed technology roadmap for RTD activities in the next Framework Programme (2003-2006) of Research and Development (FP6). These experts are drawn from industry players, academic and research institutions and civil rights organisations and cover the domains of privacy enhancing technologies, IT security, law & IT and socio-economic issues. In order to parallel the preparation of FP6 in this area, RAPID aims to deliver its results in 12 months. Efficient project management and scientific coordination structure that combines human resources and skills and state of the art quality assurance techniques will enable this ambitious timescale.

### **Objectives**

RAPID It aims to develop a state of the art trans-national collaborative environment that brings together leading experts from the privacy, identity management community, experts in technical and managerial aspects of information security, industry and end-user stakeholders, as well as policy analysts and legal scholars. The goal is to establish an active environment through which a strategic R&D roadmap can be developed. This roadmap will provide the baseline for future work and research in the domain of privacy and identity management. In order to achieve these aims, RAPID pursues the following objectives:

- 1. Community building*
- 2. Roadmapping*
- 3. Achieve consensus on RTD priorities*
- 4. Coordinate with related roadmap*

## **ESORICS NoE**

The European Symposium On Research In Computer Security (ESORICS) is the premiere conference on computer security in Europe. It brings together the foremost European experts (and indeed world experts) in the field of security, trust and privacy both at the symposia and in the Program Committee and Steering Committees.

The ESORICS Steering Committee proposes to coordinate a NoE in security under FP6 to address the challenges posed by the increasing reliance on IT. It will be based around the expertise embodied in the ESORICS community. An EoI with the support from some 40 academic institutes and industrial companies was submitted this summer.

Peter Ryan

Peter.ryan@ncl.ac.uk