

PAMPAS
Workshop on Requirements for Mobility, Privacy and Security

Trust and Trust Management

Damian Mac Randal
Business and Information Technology Department
CLRC Rutherford Appleton Laboratory
d.f.mac.randal@rl.ac.uk

The current explosion in the use of mobile devices has taken many existing privacy and security concerns out of the relatively controlled “fixed network” scenario into a much more exposed environment. It also adds further complications of its own, in particular the ad hoc nature of the “networks” being used and of the end systems being accessed. This raises specific concerns over:

- Authentication (client and provider)
- Authorization (includes billing)
- Confidentiality (of transaction existence and location.)
- Security (storage and transfer of data in an open environment)
- Accountability (of network/nodes for use of services/confidential data)
- Robustness (of interactions in an ad hoc dynamic network)
- Etc.

While some areas are receiving concentrated attention and are making reasonable progress (traffic encryption, digital signatures, roaming, micropayments, etc), one area that is still relatively underdeveloped is trust and trust management in an inherently open and ad hoc (p2p?) network environment. Issues include:

- Uncertainty/lack of knowledge about neighbouring nodes’ identities
- Limiting downstream dissemination of shared information
- Semantics (explicit and implied) in service requests/offers
- Detection and avoidance of rogue nodes

In essence, ad hoc networks and highly mobile individuals create a situation where even the imperfect privacy and security currently provided by fixed networks (corporate LAN policed by the company, public networks policed by the provider & contract law, eg GSM) is going to be impossible to achieve. Users will have to live with imperfect privacy / security and develop appropriate risk management strategies for themselves and their agents.

The Business and Information Technology Department of CLRC

(<http://www.bitd.clrc.ac.uk>) employs about 120 staff researching and developing IT, including considerable experience in EU projects funded under Esprit II, III, IV, V, Telematics, RACE and ACTS programmes. The role of BITD within CLRC focuses on the bi-directional knowledge and technology transfer between e-science and e-business.

The **ISE Group** of the **BITD-CLRC** at RAL offers IT research and development expertise using leading-edge technologies and methodologies. The focus of the group is in the design and development of IT systems which organise and deliver information within and between organisation. The distinguishing feature of the group's activities is that they involve the design and development of systems that organise and deliver information (as distinguished from data) across heterogeneous and distributed sources. The group also provides resources, consultancy and technical expertise to the **UK Regional Office of the World Wide Web Consortium** and the **e-Science Centre of CLRC**.

Relevant current projects include:

itrust Network: Trust Management in Dynamic Open systems (IST FP V). Provides a forum for cross-disciplinary investigation of the application of trust as a means of establishing security and confidence in the global computing infrastructure, recognizing trust as a crucial enabler for meaningful and mutually beneficial interactions. iTrust has been set-up with EU IST funding as a network of Centres of Excellence from both technology-oriented disciplines and the fields of law and social sciences. CLRC Rutherford Appleton Laboratory is leading the UK hub.

GRASP: Grid-like architecture for Application Service Providers (IST FP V). Exploring a new advanced system infrastructure for Application Service Provision (ASP) based on GRID technologies. CLRC/BITD in GRASP leads the design of the GRASP service-oriented architecture.

SWAD-Europe (IST FP V) supports W3C's Semantic Web initiative in Europe and will help generate future Semantic Web standards. CLRC/BITD is leading a workpackage focusing on trust infrastructures for the Semantic Web.

PELLUCID (IST FP V) aims to develop a flexible and adaptable platform to assist organisationally mobile employees in public sector organisations. Security and trust management requirements play a significant role in the design of the PELLUCID platform. CLRC/BITD coordinates this project.

CORAS (IST FP V) is developing a base framework for model-based security risk assessment by exploiting the synthesis of Risk Analysis methods with graphical Object Oriented specification methods. CLRC/BITD is involved in the modelling and method integration work of CORAS as well as leading the project's clustering activities.

TELEMAC (IST FP V) is developing a modular and reliable system supporting remote telemonitoring and telecontrol of small depollution units. Safety and security assessment is important when designing and maintaining mission critical control systems such as the TELEMAC system. CLRC/BITD is leading the architecture work.