Chapter 4.21
Trust and Security in Ambient Intelligence:
A Research Agenda for Europe

Andrea Servida
Deputy Head of Unit, European Commission, Belgium

ABSTRACT

The information society is increasingly dependent on largely distributed systems and infrastructures for life-critical and business-critical functions. The complexity of systems in information society is rapidly growing because of a number of factors like their size, their unboundness, and interdependency, the multiplicity of involved actors, the need to pursue more decentralised control and, last but not least, the growing sophistication in functionality. This trend together with the pervasive use of open information infrastructures for communications as well as of freeware software and common application platforms expose our society to new cyber vulnerabilities and threats that deserve better understanding, assessment, and control. Building trust is essential for the development of the information society, and the electronic commerce in particular. This chapter outlines the main research directions that have been defined as the priority ones in which to engage the European research community in the thematic priority Information Society Technologies (IST) of the 6th Framework Programme. To this purpose, the chapter consolidates the results and recommendations of a number of consultation workshops that were organised by the Commission in the years 2000-2002.

INTRODUCTION

Our society is increasingly dependent on communication networks and information systems. Systems are more and more open, interconnected, and interoperable. "Plug and play" and "wireless in everything" technologies allow a large variety of devices to be connected and work in the background. The legacy of enterprises and administrations will soon become essentially a digital one and, therefore, "traceability of the bits" will have

to be ensured. But while, formerly, data were just data and executable codes were just executable codes, "data" are now both "data and executable codes" and have become living and active objects. They can be downloadable software to give access to services on mobile devices, or agents acting on your behalf on the net, or multimedia content carrying with them their usage policy, and so forth. Their "semantics" can be "good," or "bad." At the same time, systems are becoming increasingly complex. They have short and diverse live cycles and require frequent updates. As a consequence, their management becomes vital. Terminals themselves become distributed and communicate: how can one verify/authenticate the various components? The boundaries of enterprises are blurring; enterprises are involved in multiple dynamic networks where information and functions are shared with others. The cosy closed enterprise is in the past: the mobile worker needs to access corporate data (B2E), suppliers get access to your design data, and you to share with them various business processes. In that context, who is an insider who is an outsider? All this brings complex security requirements at the application level.

The complexity is going to further develop in the Ambient Intelligence (Ducatel et al, 2001) vision (called in short AmI) that was developed by the Advisory Group (FP5 ISTAG, 2002) of the Information Society Technologies programme (IST Web site, 2005) in the course of the 5th Framework Programme. AmI drives and envisages the development of surrounding computing and wireless communication environments where "resources" would be available and shared. Users would be empowered through a digital environment that is aware of their presence and context, and is sensitive, adaptive, and responsive to their needs, habits, gestures, and emotions. AmI would be characterised by ubiquity, awareness, intelligence, and natural interaction. However, all developments in the AmI scenario would only be possible if they would be underpinned by novel security paradigms, concepts, models, architectures, and technologies.

As we move from the information and communication paradigm to the AmI one, we need to change our perspective to security and security technologies and look at them as key enablers to share, exploit, and manage our resources, knowledge, and values. Associated to this change, the human component would also play a key role for which we need to develop a culture of security that would make everybody understand that, in tightly interconnected and open environment of AmI, his or her security and his or her misbehaviour may be critical to the entire society. And, we would also need to better understand both the nature of vulnerabilities of the information infrastructure and the scale of its interdependencies with other societal and economic systems and infrastructures that may be part of a broader reflection on how we would like or may need to depend on advanced and volatile technology and technological platforms.

In the AmI scenario, security can be seen at different levels:

- **Securing the individual and his or her personal info sphere:** Privacy of the individual has to be guaranteed also in the virtual world. It entails confidentiality, integrity, availability of personal data, anonymity in e-vote, pseudo-anonymity when buying on the Internet, and so forth. Preserving the balance between transparency and opacity of every individual has still to be found in the virtual world: one should not get the impression that he or she is permanently tracked. At the same time, non-repudiation (who has done what) has to be guaranteed in e-business transactions.
- **Securing dynamic virtual communities:** with incoming and outgoing members that communicate through networks, which are increasingly heterogeneous and mobile. Communities should be able to choose