Workpackages

Activities and work packagesPRIAM is organized into three strongly tight work packages:

- WP1 investigates the legal implications of privacy and the possible evolutions of the regulation to cope with the new technological landscape.
- WP2 addresses the formal definition of privacy policies suitable for the ambience intelligence world.
- WP3 is a study of the implementation issues of the privacy policies in the resource constrained context of ambient intelligence. WP1: Privacy from the legal and social perspectiveThe first objective of WP1 is to investigate whether the current legal European framework with respect to privacy is suitable for the ambient intelligence world and, if not, to study the kind of adaptations or complementary provisions that would be appropriate.

In most European legislations, the citizen has the right to:

- have access to his data when it is collected by a third party,
- enforce the rectification of incorrect data,
- enforce the deletion of data in the third party’s computer or storage facility.

The intention of the legislators was obviously to protect the citizens against intrusions from governments or private companies, but the relevance of such rules in the context of spontaneous peer-to-peer networks is far from obvious (not to mention their practical feasibility). Private data still has to be legally protected though (and even more than ever), so the careful study of the foundations and the practical implications of privacy is of prime importance to establish trust in the new ambient world.

One of the outputs of WP1 will be a contribution to this study with proposals concerning the most appropriate types of regulation for privacy in ambient systems. The regulation might be administrative, deontological (legal ethics) based on the moral obligations of the actors in the system, or contractual for each of the ambient services.
WP2: Definition of privacy policies for the ambient intelligence worldSeveral frameworks have been proposed for the definition of privacy policies, especially for websites: P3P and E-P3P, for example, make it possible to express privacy statements using XML with a specific vocabulary. While inspiration can be taken from these approaches, they suffer several shortcomings (lack of preciseness or expressiveness, lack of formal definition, ambiguity, etc.) and were not designed for the exchanges of data on resource constrained devices.

Task WP2 will put forward a framework for the definition of privacy policies for the ambient world relying on the notion of accountability. This framework will be based on a “privacy policy expression language”. This language should have a clear semantics and be amenable to a realistic implementation on resource-constrained devices. In addition, this language should be expressive enough to distinguish different kinds of usages (e.g. read, play, transfer, store, etc.), conditions (time, subscription, etc.) and obligations (payment, declaration, etc.) and should be translatable into a language that can be understood by the different parties involved.
WP3: Implementation of privacy policies on the ambient intelligence architecture The goal of WP3 is to reflect on the feasibility of implementing privacy control policies and mechanisms in ambient environments, and in particular, on the techniques that need to be implemented in the software environments on ambient computing devices.

Several challenges are posed in terms of implementation. These can roughly be classified into two categories that will be addressed by PRIAM: operating system and cryptography issues.

As far as operating systems are concerned, the first concern is memory limitation. This obviously requires that audit logs record as little information as possible. This is particularly hard since the number of other devices with which a device can communicate is extremely large, so a log of interaction could become large also. On the other hand, audit logs need to contain enough information to be able to analyze for detection of violations to the privacy policies in place.

Another challenge relates to the fact that most devices will not be under the control of trustworthy authorities so physical tampering is possible. The device and its operating system must provide measures to protect the integrity and confidentiality of the audit log and of the privacy control policies. The integrity of the audit log is especially important to make it usable in court.

The lack of resources available on the ambient intelligence devices also introduces new challenges in terms of cryptography. In a context where devices are limited and geographically located, in a large-scale environment, a trade-off has to be found between efficiency and risk. A risk analysis model has to be defined considering adversaries with much more resources. New security challenges as well as open problems in cryptographic systems appear in this context.