

# Secure Ubiquitous Environments

## PAMPAS02

Javier López, Andrés Marín, Miguel Soriano  
Universidad de Málaga  
Universidad Carlos III de Madrid  
Universitat Politècnica de Catalunya

29th July 2002

Future wireless communications (3G and beyond) will lead to powerful networks in ubiquitous environments, offering new services, and hiding the complexity of the mixture of future wireless telecommunications technology. Body and personal area networks (BANs and PANs) are envisaged to be of great impact on our everyday activities, and to integrate in a seamless manner with traditional networks. Protocols and applications should share a common view on discovery/advertisement, proxying/caching, invocation, authorization, authentication and trust model. Next generation mobile services should be designed for the limited capabilities of pervasive devices like PDAs, handheld PCs, embedded computers and mobile phones. This leads us to the following propositions:

- cost/efficiency trade off with respect to partly limited bandwidth in the use of networks has to be addressed at the same level as the service management, via smart caching;
- personalisation is paramount for services, data and devices. User profiling and personal assistants are invaluable for the user and for 'value added' companies, they should be also addressed at the same level as service management;
- adaption of user interfaces has to be considered for each individual device in order to efficiently communicate with services/people and to control/monitor other devices. Due to lack of standards and the completely different hardware and software properties like display size, loud speaker, voice recognition etc, content and control has to be individually adapted for each device, user and application.
- tamper-proof hardware crypto tokens (i.e. as smartcards) should be the base of the security and authentication demands including biometrical user identification (e.g., fingerprint and facial information) and authorization as well as profile management – multifunctional smartcard provide basis for security in private networks as well as business networks in order to manage data with intellectual property rights.
- security requirements in this environment include among others the following: Single Sign-On (SSO), support for multidomain trust policies and authorization, cryptographic processing, secure application-based transaction management, and uniform credentials and certification infrastructure.

In ubiquitous networks, it is necessary a mechanism to let users have seamless, transparent and trusted access to the network resources. The SSO mechanism allows a user to perform only an initial authentication and authorization in order to permit him/her access to resources, without the need to authenticate or authorize subsequent times. Deploying mechanisms such as SSO in this environment imply a great complexity and the traditional authorization solutions based on

PKI authentication plus Access Control Lists (ACLs) have important scalability problems. To overcome these problems, a new generation of infrastructures is needed, including Authentication and Authorization Infrastructures (AAIs), management of Attribute Certificates (ACs) and new mechanisms for privilege delegation and revocation.

To enable users to connect to any network access provider, whatever the provider of the subscription may be, an inter-domain security infrastructures like AAA (Authentication, Authorization, Accounting) should be used. For this AAA-like infrastructure to remain independent of the access network technology, a generic protocol named PANA (Protocol for carrying Authentication for Network Access) is currently being defined by IETF.

Moreover, the discovery/advertisement phase is very important when nodes in a network are changing their placing. An incoming node must find out where to connect to the net and should notify its position to the others members in the network. In the same way, an existing node should advertise to the world whether it is an access point to the net or not. These mechanisms become more involved when nodes are continuously in motion because of handovers and roaming. In such scenarios, and where the involved parties are limited capabilities devices, the minimization of bandwidth usage and computation is critical. Current works in other areas such as multicast security rekeying allows a node to join or leave a group with a minimum number of protocol messages. These messages are intended to update the network state and deliver a shared secret in order to achieve group privacy. The development of multicast-like architectures and protocols for ubiquitous networks which enable secure discovery and advertisement messages is a topic of interest.

Among the computation models, autonomous and collaborative agents are the best suited for such an heterogenous environment. Despite its benefits, working with agents raises some serious security issues, especially if they are mobile agents. Protection of hosts from hostile code and protection of agents while traversing untrusted networks can be performed by well-known cryptographic protocols. But there is no effective solution to protect the agent against a hostile site, i.e. the problem of malicious hosts as it is known. Mechanisms to assure the integrity and privacy of agents have to be performed in ubiquitous environments in order to solve the problem of malicious host without losing the benefits of a mobile agent system.

In general, we are interested in the development of architectures and protocols for ubiquitous environments which enable user-centered services, specially in the fore-mentioned security requirements. There are a number of emerging networks beyond 3G that could benefit from an approach like ours, for example: mixed ad hoc/infrastructure networks, smart environments and sensor networks, networks providing location-dependent wireless services, home networks, infrastructure networks, spontaneous networks of people engaging in a common activity for work and leisure, smart spaces equipped with lots of cheap sensors and actuators, or networks of vehicles on the highway keeping track of each other and influencing each other for safety reasons. There are plenty of potential application areas for this project including tourism, financial applications, ticketing/subscription, pricing, account charging, communities and entertainment, gaming, education, health care, collaborative work in virtual organizations, mobile support, remote monitoring and maintenance, private home networks, private data storage, knowledge management, advanced process control support, and enterprise applications.