

# The need for security solutions in ad hoc connected portable communication and storage devices

Position paper of Philips Electronics N.V. for the PAMPAS Workshop on Requirements for Mobile Privacy & Security

Author: Claudine V. Conrado

The new era of ubiquitous computing brings to users a vast amount of information and personalised services through a number of diverse, integrated and surrounding computing devices, independent of time and location. The trend towards ubiquitous computing is also represented in the trend towards dynamic or ad hoc networks as well as mobile/wireless communication technologies and services. In the near future, it is expected that portable devices which are capable of supporting wireless peer-to-peer and ad hoc interaction, as well as storage, will grow in popularity.

The trend described above opens up a large number of new opportunities for services and applications in the mobile/wireless domain. The distribution and exchange of content of any type by means of portable devices connected in a wireless and ad hoc manner is seen as one of such relevant novel applications. This opportunity is indicated by the tremendous growth in the distribution and exchange of content via the Internet that has been seen over the past few years. Moreover, the possibility to store content in such portable devices is seen as an essential feature of the application.

One possible scenario is that of a small personal portable device which can be carried by a user wherever he/she goes. The device contains high speed wireless digital interfaces to allow communication with other devices, as well as a small LCD screen, loudspeakers with a connection for headphones and a large amount of storage space. In this way, users can carry with them stored audio-visual content, which they can easily access by means of the device. In addition, users can also store, for instance, their user profile data reflecting their tastes and preferences concerning any type of content.

In such a scenario, when users possessing the portable devices meet, for instance, in a public space, they may exchange any piece of content that is stored with either of them by means of an ad hoc wireless connection between their devices. Moreover, a user may obtain from another user only those pieces of content which match his/her profile of preferences. In this case the devices must communicate with one another in order to compare the profile of one user, stored in his/her device, to the set of contents from the other user, stored in the other device.

From such scenario of usage of wirelessly connected portable devices with storage capabilities which was described above, a number of security-related issues emerge. In order for this scenario to satisfy content providers and content owners, copyright issues will have to be dealt with during the exchange of content between users. Therefore, the user's rights relating to a piece of copyrighted content is yet another type of data which may have to be stored along with that content, and proper content protection and rights management policies will have to be in place.

From the users' side, the main security requirements that emerge from the above scenario relate to the protection of their privacy in all interactions. This is especially the case in the interactions in which personal content is exchanged. A special case of a user's personal content is his/her user profile data. In the situation in which a user's profile is to be compared to a set of content items in another user's device in order to find possible matches, a mechanism must be in place that ensures the privacy of the profile data, particularly in case no matches are found.

The security requirements in wireless and ad hoc networks described above pose new challenges to security technology. One of such challenges relates to the limited computing capability of many of the end devices which limits the system's resources that can be dedicated to security computations. A further challenge relates to the high vulnerability of wireless connections to attacks, such as Denial of Service, and to failures in general, which may be of a non-malicious nature. Such challenges make security requirements for wireless networks much more demanding than those for static wired networks.

Concerning Digital Rights Management, there are a number of solutions for conditional access as well as copy control functionality for pay-applications on the Internet and IT world. Where appropriate, such solutions should be adapted to the context of mobile and ad hoc networks, and where needed, new cryptographic technology should be developed in order to tackle the specific challenges.

More specifically, in order to support the secure distribution, exchange and storage of content by means of portable devices connected in a wireless and ad hoc manner, a number of security functions are required, which include:

- authentication of devices/users, in order to support the management of identities and closed groups,
- users' privacy for communication and personal data,
- content encryption and integrity,
- key management.

The identification of the appropriate solutions will depend on criteria such as which security functions are required in a given context and the existence or not of a central certification authority.

Technology alone will not provide the full solutions to all challenges in wirelessly connected ad hoc networks. Legislation, together with enforcing mechanisms, will always play an important role in such solutions. However, truly effective security protection in the wireless/mobile context will require the design and implementation of systems with technological built-in security policies.