The relationship between hardware design and software level security in highly dynamic mobile ad hoc networks

Serge Chaumette
Professeur, LaBRI, Université Bordeaux 1
Responsable de l'équipe Langages, Systèmes et Réseau (LSR)
Responsable du thème Mobilité, Ubiquité, Sécurité (Muse) de l'équipe LSR

There is no doubt that *The Internet of Things* will be a major dimension of our future life. Today, many mobile types of equipments are connected, and tomorrow, our whole environment will be equipped with sensors and smart devices that will self-organize as Mobile Ad hoc Networks. One of the major characteristics of these networks is that they are highly unstable: they create dynamically, they get split and connected again depending on the movements of their composing devices, and the devices can join and leave in an expected manner. The applications that target these configurations must thus be specifically designed to support this dynamicity, still ensuring a high level of security in this unstable framework.

The topic of this talk is the impact of hardware design on software/communication level security.

More precisely, there are two questions that are closely related to the relationship between hardware design and software: (i) how to support secure operations on a device that is not necessarily under the control of a trusted person? (ii) how to secure communication, communication protocols and the associated applications.

The first issue is dealt with by embedding a Trusted Platform Module (TPM), such as a SIM or a dedicated Smart Card (for instance a micro-SD Java Card). A piece of software can then be uploaded inside the TPM and is thus protected from any malicious behaviour. Even though this is a really difficult issue for hardware designers, once available, it is quite simple from a software level point of view: the problem resumes to storing specific cryptographic keys inside the TPM of each mobile device. To achieve this goal, a number of approaches exist that we will describe in this talk. We will focus on an original approach based on a group security policy that we have designed and implemented. We will also discuss reconfigurable hardware that could be used to provide different levels of security depending on the context and on the applications requirements.

The second issue is how to secure communication, communication protocols and the applications that use them. Seen from a software level perspective, securing the data to transfer is straightforward once cryptographic keys are available. Securing the communication protocol itself is much more difficult. Even though the messages can be handled and thus ciphered inside the TPM, the effective communication is not achieved by the TPM itself but uses some external radio chip. This is typical of a SIM plus NFC configuration. The risks that arise relate to both malicious device owners and insecure operation environments. The questions are for instance: how to ensure confidentiality? How to lower if not suppress the impact of replay or man in the middle attacks? Etc. It appears that providing a secure hardware link between the TPM and the communication chip not only ensures confidentiality regarding a possible malicious device owner but also makes it possible to ensure some guaranties even though the mobile operates in an insecure environment. We will illustrate this point by means of examples.