Trusted Computing for Mobile Cloud computing

Résumé du projet de recherche (Langue 1)

Since Google added support for Near Field Communication (NFC) technology to their Android operating system and to their Nexus devices in 2010, the number of smartphones equipped with NFC functionality is rapidly increasing. Hence, there is a concomitant need to secure these phones against vulnerabilities that arise from each additional application. Moreover, several applications together can expose the smartphone to new security weaknesses, especially when the smartphone externalizes its resources within a Cloud computing. Regarding local computing and processing capabilities, and high-speed wireless networking features, smartphones (or mobile devices referred in later contents) will overtake PCs as the most popular Web access devices by 2013, as predicted by Gartner. By the end of this decade a significant fraction of web access (from fixed or mobile devices) will be to mobile services and resources. This is because many of our queries are about the world surrounding us, and mobile agents (people, vehicles, robots) are the ideal probes of people and their environment. Moreover, the data of interest (e.g., video data) may be scattered across many mobile observers, and thus require in loco data aggregation and query resolution using software specialized for the local context. These mobile agents effectively form a Mobile Cloud by integrating mobile devices into existing Internet Cloud computing infrastructure. In the context of the mobile cloud computing, each mobile device is a service provider vis-à-vis to the cloud and depends on the computing on the cloud and its own physical device. As a service provider, a mobile device can provide sensing services (context-aware for mobile devices and neighboring environments), computing service (mobile phones become more powerful, however with energy restrictions), communication service (serves as an information gateway), and storage service (needs to consider backup/restore, sharing, etc.). In the cloud, each mobile device has an extended semi-shadow image (ESSI) that must provide a trust environment to cooperate with the trust environment of the physical device to allow access to services in a secure manner. The trust environment may rely on the TEE/TPM that can be based on a physical secure element or a virtual one. The objective of this thesis is two fold. First, a trust model for NFC smartphones should be defined. It must be based on the secure element of the smartphones to guarantee data/application integrity and the authentication of the user. Second, since that the smartphones are extended with the Cloud resources, security issues must be considered in the context of the mobile cloud computing. A general security model should be designed by extending the local trust model of the mobile devices. The proposed trust model should be validated using formal-method tools.