Software security in embedded systems

Résumé du projet de recherche (Langue 1)

As the Internet of Things becomes a reality the trustworthiness of all its components assumes the utmost importance. The trustworthiness of any system security, reliability etc. depends on its weakest part. When wireless sensor nodes (WSN) are included in the Internet of Things then it is likely that one of the more vulnerable parts will be the wireless sensor nodes themselves. Those devices are actually nowadays deployed in a number of applications, critical infrastructures, smart grids, medical devices, all with their particularities, however the trend is that they all tend to be more and more connected trough wired or wireless links and all rely on low-end and cheap micro-controllers. These devices can be attacked by “standard” network based approaches but also by physical means if they are left unattended in remote sites which is, after all, the preferred application for WSN. While much research effort has been spent on improving their network security, the protection of the nodes and especially their protection against software and attacks has been, until now, neglected. We are convinced that protecting those devices is essential since compromised nodes put the whole system at risk. This thesis aims to significantly improve the trustworthiness of such devices. To achieve this goal we will investigate novel attacks, appropriate counter measures and protection mechanisms, while also considering the severe constraints of energy and silicon area.

Résumé du projet de recherche (Langue 2)

In particular we will focus on: an attack resistant system architecture how to make systems resilient to vulnerabilities and build secure low level services. work on automated analysis and new techniques and methods to experimentally validate such systems. For example new mechanisms for finding bugs of proving their absence in [2]. It is foreseen that a whole system may be evaluated by relying on symbolic execution to discover invalid execution paths (e.g. using [1]). The range of protection mechanisms will be also evaluate in the context of the Tampres project where devices will be manufactured (by NXP and IHP) this will be used to evaluate the results. References [1] V. Chipounov, V. Kuznetsov, and G. Candea. The s2e platform: Design, implementation, and applications. ACM Trans. Comput. Syst., 30(1):2:1–2:49, Feb. 2012. [2] K. El Defrawy, A. Francillon, D. Perito, and G. Tsudik. SMART: Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust. In Proceedings of the Network and Distributed System Security Symposium, NDSS 2012, San Diego, 2012.