Thesis subject:

Internet of Things security: towards a robust interaction of Systems of Systems

PhD Advisor:

Yacine Challal : Maître de Conférences, HDR (Associate Professor)
Tel: +33 344.234.429, email: ychallal@hds.utc.fr

Context of the thesis :

The thesis is part of the project activities of the Laboratory of Excellence (LABEX) at the Université de Technologie de Compiègne (UTC) in France on the Control of Technological Systems of Systems (MS2T) (www.utc.fr/labexms2t).

Internet of Things (IoT) is an enabling technology for Cyber-Physical Systems or Systems of Systems. Indeed, Internet is evolving from a network of personal computers and servers toward a huge network interconnecting billions of smart communicating objects. These objects will be integrated into complex systems and use sensors and actuators to observe and interact with their physical environment, and hence allowing interaction among autonomous systems.

PhD thesis description:

IoT raises important questions and introduces new challenges for the security of systems and processes and the privacy of individuals. Some IoT applications are tightly linked to sensitive infrastructures and strategic services such as the distribution of water and electricity and the surveillance of bridges and buildings. Other applications handle sensitive information about people, such as their location and movements, or their health and purchasing preferences. Confidence in and acceptance of IoT will depend on the protection it provides to people's privacy and the levels of security it guarantees to systems and processes.

An urgent prerequisite for securing IoT is the development of *efficient security mechanisms for tiny embedded networks* with scarce resources. Current developments in wireless sensor and actuator networks, RFID technology, mobile computing and so forth, demonstrate the resource scarcity of the devices and technologies that will be part of IoT. The ubiquitous nature of IoT raises legitimate questions about the privacy of persons, and how to cope with the heterogeneity of user and application requirements in terms of security services. This requires the development of *adaptive, context-aware and user-centric security solutions*.

This thesis aims to develop a new global approach for IoT security that takes into consideration the involvement of smart communicating objects in the control of complex systems and the ubiquitous nature of IoT. Security requirements in System of Systems interactions will depend on the context that evolves in space and time. Therefore, security policy definition and enforcement should be adaptive and "context-aware". This will allow the development of efficient security solutions for robust interaction of smart objects with persons, the technological ecosystem and control processes, while providing autonomy for objects to *safely* perceive and act on their environment.

References:

[1] Rodrigo Roman, Pablo Najera, and Javier Lopez, « Securing the Internet of Things », IEEE Computer, vol. 44, no. 9, pp. 51-58, September 2011

[2] Tobias Heer, Oscar Garcia-Morchony, René Hummen, Sye Loong Keoh, Sandeep S. Kumar, and Klaus Wehrle, "Security Challenges in the IP-based Internet of Things", Wireless Personal Communications (Springer), Volume 61, Issue 3, pp 527-542, December 2011.