Title: Key Security Challenges in Smart Swarm of Things (SSoT)

Authors: Oscar Garcia-Morchon, Sye-Loong Keoh, Sandeep S. Kumar
Philips Research Europe

Emerging Technology Space: Internet of Things, Sensor and Lighting & Building networks, Smart Cities

Class of Cryptographic Requirements: Lightweight Cryptography, key establishment/agreement/management

Abstract:
The need for energy and operational efficiency in cities has resulted in an explosive deployment of smart applications for surveillance, intelligent building control automation and ubiquitous sensing in smart cities. This is leading to a proliferation of interconnected devices, creating a so called Smart Swarm of Things (SSoT). The SSoT consists of resource constrained devices (typically multi-vendor and under multi-user control) that work cooperatively towards fulfilling a task, and it requires continuous exchange of information over different communication technologies such as IP, BacNet or ZigBee.

Key agreement/establishment, identification and authentication of devices are key to ensure secure interaction between devices in SSoT. They remain as a challenge mainly because devices do not have a priori knowledge of each other, hence exacerbating the difficulty in key bootstrapping process. Furthermore, the lack of computational and memory resources restricts the usage of asymmetric-cryptography, instead solutions based on pre-shared keys such as DTLS-PSK in IETF CoAP Protocol have been proposed. However, the management of a huge number of symmetric-keys is not trivial due to scalability problems of a centralized solution and a lack of suitable distributed solutions.

An identity-based method for direct generation of pairwise symmetric-keys between peers is required for SSoT. Such an approach must be lightweight and efficient both in terms of computation and memory, while allowing for easy provisioning and establishment of secure channels between interacting devices. The availability of such a secure cryptographic primitive would mean an efficient approach for a device to generate the pairwise symmetric-keys with all other devices in a network; thus, allowing for efficient device identification and authentication in a large SSoT. Such an approach would speed up operation since access to an online key distribution center is not required anymore, while computationally it allows for distributed key agreement without the need of asymmetric-cryptography