## Title: Towards a Generic Trust Platform For Smart City and IoT Applications

Speaker: Dr. Nabil Abdennadher, Full Professor, University of Applied Sciences, Western Switzerland

Abstract:

Smart City consists on deploying electronic Internet of things (IoT) devices, at a city scale, to collect data and then, use these data to manage assets and resources efficiently. Today, most of these devices are installed and managed by local authorities. However, in the near future, we can expect that these devices belong to the citizen. Several use-cases have already come to light. Initiatives such as Smart Geneva, by the State of Geneva, aims specifically at creating a smart city open data solution.

The desire to allow the citizen to connect his own device reveals at least three challenges:

- How to convince the citizen to connect his device?
- How to secure the connected devices from any malicious action ?
- How to trust a device that does not belong to the "authority", or simply a device whose behaviour is not predictable?

This talk deals with the third challenge.

IoT devices are often subject to misbehaviour resulting from the poor quality/performance of devices or from external disturbances (e.g. cyber-attacks, physical attacks, physical obstructions, etc.). Our goal is to detect misbehaving devices and assign a low trust score to the data they are sending.

This talk proposes a generic trust framework used by IoT applications to assess trust rates of IoT devices. The developed framework targets non-critical IoT applications with no "legal security issues". Non-critical applications do not have strict security policies or legal issues and are tolerable to a margin of error.

The framework assesses the "trustworthiness" of data retrieved from IoT devices, in order to deduce their reliability. The trust score assigned to a data (received from a given IoT device) is used to make necessary "arrangements": isolate the IoT device, fix the problem, etc.

To calculate the trust of data collected by a given device, we represent sensors by a set of features. Each feature expresses a given characteristic of the sensor that could affect its trustworthiness. The nature and number of features depend on the device's type. For each collected data, a score related to a given parameter is processed. A global data quality score, modelling the trustworthiness of the collected data, is then calculated.

The framework is being evaluated in the case of 1'000 noise sensors installed in Carouge (Geneva Canton). The goal is to draw up the traffic noise map of the city.

With its ability to assess trust, integrity and quality assessment of the data it collects, this generic trust framework for IoT applications will contribute to ensuring that data provided is dependable and trustworthy. The result will be tangible citizen benefits. With information delivered in pseudo real-time, a new generation of services and policies will be possible, with the ultimate aim of improving our citizen way of life and providing our democracies with high quality open data to inform its decisions.