ABSTRACT #1

Title: Cryptography for Highly Constrained Networks

Presenter: Dr. René Struik**,** Struik Security Consultancy, Toronto, ON Canada

Emerging technology space: Ubiquitous security, smart objects, “Internet of Things”
Cryptographic requirements: Performance, resource, and device cost constraints; security, ease of provisioning, flexibility of deployment.

Abstract:
Recent years have witnessed a surge of interest in general-purpose, self-organizing, multi-hop ad-hoc networks. Wireless communications between static and moving devices in these networks are typically based on radio transmissions, often operating in unlicensed frequency bands, such as 868/915 MHz and 2.4 GHz, and might involve single-hop or multi-hop message routing. From a security perspective, wireless ad-hoc networks are no other than 802.11 WLAN or any other wireless network, in that these are vulnerable to passive eavesdropping attacks. The very nature of ad-hoc networks and cost objectives for these impose additional security constraints, however, which make these networks difficult to secure: devices are low-cost, with limited capabilities, in terms of computing power, available storage, and energy-drain, and cannot be assumed to have a trusted computing base aboard, nor a high-quality random number generator; communications cannot rely on the online availability of a fixed infrastructure and might involve short-term relationships between devices that may never have met before (so-called promiscuous behaviour). These constraints severely limit the choice of cryptographic algorithms and protocols and do influence the design of the security architecture, since the establishment and maintenance of trust relationships between devices needs to be addressed with care. In addition, battery lifetime and cost constraints put severe limits on the security overhead these networks can tolerate, something that is of far less concern with higher bandwidth networks, such as 802.11 WLAN.

We discuss security architectural design elements for constrained networks and highlight areas where conventional cryptographic approaches may fall short, such as with public key lifecycle management, symmetric-key crypto overhead, and support for flexible trust models, and points towards solutions. Discussion is illustrated using deployment scenarios with ZigBee, w/HART, Body Area Networks, and the Smart Grid.