Saal: 22:30 01:00 Day: 4 Track: Security & Hacking nA
Simulacron-3

Title: **Attacking IoT Telemetry**

Subtitle: A study of weaknesses in the pipeline of rapidly advancing sensory development

Speaker: **Michael Schloh von Bennewitz**

Short: *In this hour long presentation, we consider weaknesses in the pipeline of advancing sensor developments and demonstrate passive and active attacks on hypothetical critical infrastructure using real sensor devices. This presentation does not use scare tactics, but rather hacks along in a playful and humorous way.*

Long: We study three models of IoT system design, machine to machine (M2M), human to machine (H2M), and a hybrid M2M/H2M, considering attack vectors of each. We move to media, examining weak points in Bluetooth, WiFi, and copper cabled connectivity with mention to IPv6, ZigBee, and RFID as well. We cover typical protocols of IoT communications when collecting telemetry data and passing it on to a message bus. Moving to the science of telemetry, a field study illustrates typical use cases for sensor data collection. We wrap up by considering the points of weakness of a sensor connected critical infrastructure. Demonstrations of Bluetooth sensor communication, message publishing, server and architecture inspection, packet captures, and reverse engineering serve to illustrate the topics at hand. Attacks using Ubertooth, WiFi Pineapples, and LAN tap demonstrate the weakness of existing products.