Title: On the Integration of Federated Identity Management in M2M middleware in Industrial Control Systems

Author: Youakim Badr, LIRIS, INSA de Lyon

Abstract

In the context of Internet of Things, Machine-to-Machine (M2M) middleware allows wireless and wired devices to communicate at a large-scale. M2M can also cover the case of integrating heterogeneous industrial automation systems and embedded devices distributed within and across geographically dispersed sites (grid power, transport, agriculture, smart cities, etc.). In such open boundary environments, M2M communication protocols (e.g., SCADA, UPnP, COAP, DPWS) have specific requirements and security aspects, which cannot be handled with security policies, authorization and authentication techniques developed for Internet protocols and user applications. Nevertheless, security mechanisms must give a high level of protection not only at the M2M level but also ensure authorization and authentication techniques at the fine-grained level of devices within and across different security domains. In this presentation, we present preliminary results of integrating federate identity management into M2M middleware to have common set of policies and protocols, managing the identity and trust into devices and control systems within a security domain and across multiple distinct security domains.

Download the presentation