Thoughts on IoT Semantic Interoperability

Scope of security issues

Erik Nordmark

There are many pieces to the IoT puzzle ranging from radios and associated MAC protocols, via layer-3 protocols and RPC/ReST to the information and datamodels for the application data. However, in parallel with that there is a strong need for security for the IoT devices and associated infrastructure.

The security needs to encompas not only the communication security aspects of authentication, authorization, confidentiality, etc but also issues around the software lifecycle for the IoT devices; issues that we traditionally have left outside of protocol standardization. For example, in most cases there has to be mechanisms for secure software update in order to enable the device manufacturers to correct security bugs in their software. While such mechanisms need to prevent unauthorized software updates, they might also need to handle the case when the original device manufacturer seizes operation and some other entity takes over software maintenance. How would one manage the policies for who can update the software in such a case?

As IoT devices see broader deployment we might also see different types of resource exhaustion DoS attacks taking advantage of limited processing, memory, or battery capacity of the devices. While the devices would have some autonomous approaches to limit the impact of DoS attacks, one can be more effective in detecting and mitigating such attacks if the devices could report suspect or unusual traffic, combined with the infrastructure to collect and share such information across different stakeholders.

The above example areas of security are complex in that they encompass the standards for communication security, the software implementation on the devices, software implementations in the cloud and on controllers and gateways, authorization policies, relationships between the device manufacturers and the owners/deployers of the devices.

While there is collective experience in this area for devices with screens and input devices, the approaches might need to be quite different for IoT devices which might have no such input or output and which might not even be physically accessible by their owners.

In the context of the semantic interoperability workshop it would be useful to look at data models for describing the policies and mechanisms for security including software lifecycle management and automated reporting of security events. If we can find a way to leverage the expertise across the different organizations there is potential to make progress on security for IoT.