Position Paper – Barry Leiba <barryleiba@computer.org>

As the Internet of Things adds a great many devices to the Internet, a number of basic interoperability issues arise:

- Discoverability

  - How do the devices find the controllers or peer networks they need?

  - How do the controllers or peer networks find and register new devices?

  - How are devices identified?

  - Is it necessary to have anonymous / pseudonymous devices, and how does that work?

- Authentication and access control / trust

  - How do we decide to accept new devices?

  - What do we allow new devices to do?

  - Do we trust the data produced by new sensors?

  - How do we prevent attacks?

- Capability / function

  - How do devices communicate what they do and what their limitations are?

  - How do controllers restrict devices -- limit them to a subset of their capabilities?

  - How do devices interact when their capabilities are related / complementary?

That's just the tip of the iceberg, of course, but we have to start a discussion of the models for answering those questions, on which we can build the necessary protocols to manage networks of IoT devices and to have the devices interoperate.

For a long time, I've considered a basic scenario:
I have an early meeting tomorrow at an office I don't usually work in.
The meeting is on my calendar, along with its location.
My alarm clock automatically sets itself to wake me earlier.
My coffee maker starts the coffee earlier.
My car's navigation system gets the location and automatically sets my route.
...and so on...

The issues above fit directly into that scenario:
How do my calendar, alarm clock, coffee maker, and nav systen get tied in together? What are the security and privacy issues of that? How is everything coordinated? How do I, the human user, fit

into the control system? How do I keep track of the devices involved? How do we make sure it's really my calendar resetting my clock and nav system?