Key Semantic Interoperability Gaps in the Internet-of-Things Meta-Models

Ned Smith	Jeff Sedayao	Claire Vishik
Intel	Intel	Intel
ned.smith@intel.com	Jeff.Sedayao@intel.com	Claire.Vishik@intel.com

1 Introduction

The Internet-of-Things (IoT) may be described as a network of networks, but more correctly as an interoperating system of diverse physical and cyber systems. We surveyed a number of IoT systems [1] and in the process, uncovered key issues with semantic interoperability. This paper identifies areas like scope, object definition, and connectivity that we contend must be addressed in a comprehensive IoT meta-model. While we looked at a number of IoT frameworks and how they define data models, we focus on the Project Haystack [2], a 'tagging' IoT framework and meta-model oriented toward building automation but contains concepts that can be extended into other environments.

2 IoT Meta Model and Scoping

Project Haystack defines a meta model based on tagging of form **<tag>: <value>** where value contains instance data and tag defines its semantics. Several atomic tag types are defined such as Bool, Number, Str, Uri, and ID. Haystack assumes that individual buildings/sites will be highly customized, so different designers may select the same tag names but with different semantics. Semantic interoperability will require mapping of tag semantics across domains. Resolving these differences may require scope definition, a domain-of-interpretation providing the context for semantic interoperability. While in theory, the global community could define all tags and their semantics; such an approach seems too bureaucratic and impractical. A better approach may be to enable machine interpretation of tag entailment semantics through ontologies. But there is no single authority for ontology definitions hence tag entailment should include an ontology authority. The authors also suggest that blockchain may be an appropriate method for recognizing an ontology authority. Hence a tag entailment may have the form:

<tag> <ontology> <authority> <blockchain>

A **<scope>** tag may be an appropriate addition to the Haystack meta-model. Specifying a *project-haystak.org* as the local scope means tags defined by *project-haystack.org* inherit tag entailment from a *domain of interpretation* environment.. The allows locally scoped tags to expressed simply as **<tag>:<value>** pairs rather than the fully qualified **<tag> <ontology> <authority> <blockchain>:<value>**.

Just as organizations have evolved private address spaces, private DNS spaces, and intranets that take precedence over external equivalents, it is likely that objects will be locally defined having local semantics that take precedence over external equivalents. Without additional tags, Haystack does not have this functionality.

3 Everything-is-a-Cloud Meta Model including Data, Code, and Other virtual Objects

An IoT meta-model should consider enable the composition and use of many different kinds of things, including virtual objects such as data, data stores, and code. If a fundamental property of 'things' includes an identity, a credential (for proving identity) and a method for being introduced to another

'thing' a basic framework for composition exists. Haystack could easily describe virtual objects by defining additional tags. But additional tagging may not go far enough toward modeling IoT which may best be characterized as being a *network of networks*. We suggest an *everything-is-a-cloud* meta model is an appropriate extension to Haystack that comprehends scoping, domain-of-interpretation and domain-of-operation.

Realms are an explicit declaration of the system or sub-system domain-of-operation to which, resource ownership, authority, naming, and other context may be applied. Realms allow different parts of the system to have different scoping, interpretation and operation. Concepts such as device ownership, commissioning, on-boarding and guest access can be considered in the context of realm assignment.

Realms align conceptually with the 'local cloud' idea described here [3]. This concept asserts multiple devices function as part of a local independent cloud but has shared global functionality in a parent cloud. The IoTivity resource model [4] supports the notion that a 'device' is a collection of resources where a collection is recursively a resource. Intuitively, a refrigerator is a device that may consist of a collection of other devices (compressor, power supply, sensors) and these resources may further be decomposed into more primitive resources. The IoTivity resource model may be extended in the opposite direction as well, where a collection may reference resources (aka devices) outside the physical confines of the refrigerator skins, such as a thermostat or location sensor. However, IoTivity doesn't formalize the notion of domain-of-interpretation, domain-of-operation and scoping rules from which collections and resources derive context; something the authors assert are properties of realms.

4 Defining Inter-Realm connectivity

In a single network paradigm, the network architecture largely defines the device naming (e.g. IP address) and partitioning (sub-net addressing and routing) model. In a multi-network model, the gateway largely defines device partitioning. It may be difficult to describe devices and partitioning using a common naming convention and syntax due to a dependence on network layer naming and partitioning semantics "getting in the way".

Some frameworks such as IoTivity abstract device addresses by assigning devices a UUID. UUIDs are not directly routable through multiple networks. The framework must therefore provide UUID-to-network address translation; which essentially is a two-stage methodology (e.g. Step-1: map network-A address to UUID; Step-2: map UUID to network-B address). Nevertheless, the meta-model will need to describe network layer attributes insofar as addressing, routing and layered security must be exposed in order to ensure safe, reliable, protected and efficient interoperation across multiple networks.

5 Security in the IoT Meta-Model

A tagging meta-model is helpful as a mechanism for identifying network layer specific attributes and relying on gateway intelligence to perform the translation. End-to-end security requires semantic agreement between all the security management infrastructures (trusted gateways) that occupy the hops across intermediate networks in route to an endpoint destination. Even with end-to-end security semantics being worked out, mechanisms for enforcing security may differ across multiple networks. Endpoint environments likely are incapable of dealing with the added complexity of multi-hop security.

An IoT meta-model should position a common security management scheme as a system component that should be retooled first as part of an evolution of brownfield IoT networks to semantic aware IoT networks. Common security management should be an essential part of the IoT meta-model. While some frameworks allow the specification of access control, others like Haystack have no direct method

of specifying this. Haystack can be easily fixed with the addition of more tags. Information hiding can facilitate privacy, safety and security goals.

6 A Role for Object Registries

An IoT meta-model that doesn't depend on the network layers for information hiding should also not depend on them for discovery. UUID based 'device' abstraction may be insufficient in characterizing what should be hidden or discovered. The IoTivity resource model seems better, but not as good as a nested cloud model where adding resolution to the data is synonymous with discovery of a next layer of devices, resources or objects. This suggests, given an 'everything-is-a-cloud' model, that every cloud of IoT devices should have a registry describing discoverable objects. A registry is a collection of tagged values, which resonates with the Haystack meta-model. Other frameworks have ways of registering devices, but no explicit way of making that information discoverable across different realms. A registry could make the happen easily.

Other advantages of registries include the ability to map UUID's to network addresses, storage of object meta-data including access control for security. Registry systems like the Digital Object identifier system [5] have been experimented with for use with describing IoT devices [6] and have been used extensively for registering nonphysical items like films [7], datasets [8], and technical papers.

7 Summary

Semantic interoperability of IoT depends heavily on a flexible, simple yet effective meta-model. A tag-value model such as that proposed by Project-Haystack appears to satisfy these criteria, but not fully. Tags should have semantic entailment that better addresses naming given disparate parallel evolution paths. Tags should be linked to ontological bases for machine-directed semantic interpretation. A tag-value meta-model should be augmented by an 'everything-is-a-cloud' meta-model that describes not only a network of networks but also a network of things consisting of collections of other things including data and code. Security management interoperability appears to be the most significant set of functionality that should be common across all IoT networks. The use of semantically rich object registries that are machine-readable can be useful in filling the gaps we identified.

8 REFERENCES

[1] Derhamy, Hasan, et al. "A survey of commercial frameworks for the Internet of Things." Emerging Technologies & Factory Automation (ETFA), 2015 IEEE 20th Conference on. IEEE, 2015.
[2] Project Haystack: http://project-haystack.org/
[3] P. Varga, F. Blomstedt, L. L. Ferreira, J. Eliasson, M. Johansson, and J. Delsing, "Making system of systems interoperable - the core components of the arrowhead technology framework (accepted for publication)," IEEE Internet of Things Journal, August 2015
[4] Home iotivity. IoTivity. [Online]. Available: https://www.iotivity.org/
[5] https://www.doi.org/hb.html
[6] http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_EU-China_IoT_Identification_Final.pdf
[7] http://eidr.org/
[8] https://www.datacite.org/