

## **FIA session S.II.3 – Internet of Things (IoT) and the Future Internet**

**Session summary (Authors: J. Clarke, R. Roman, N. Papanikolaou, N. Wainwright, et al.)**

Main Session Goals: to highlight aspects of IoT architecture – how it should map to the Future Internet (Panel 1), and an analysis of security, privacy and trust challenges for the integration of the IoT into FI (Panel 2). See [1] for full session organisers information and further details.

### **Panel 1. IoT/FI architecture and integration (A. Bassi, S. Haller, D. Uckelmann)**

The definitions and examples of the nature of the *things* in the IoT were presented; the *things* are not the computational devices, but the physical entities (e.g. human beings, cars, trees). Devices enable the physical entities to belong to and interact with the IoT. Aspects of the IoT were summarized by how the IoT can be defined (*envision*), making use of what we have (*extend*), finding solutions that bring the IoT to the real world (*enable*), bring users to the IoT (*excite*) and generate IoT business models (*evaluate*). The challenges for IoT in the FI include those related to connectivity, services (infrastructures, protocols, deployment), interoperability (technical and semantic) and business models.

### **Panel 2. IoT/FI privacy, security & trust (T. Peirce, O. Garcia-Morchon, A. Skarmeta)**

Ongoing work in the IERC cluster covers defining the technologies of the IoT and contributions to European policies and approaches. Use cases and security *requirements* were presented, and the consequent challenges to providing IoT security. The importance of diverse human roles and interactions in the IoT environment must be emphasised in the development of security solutions. Requirements for such interoperability, applicability, and optimality (against constraints) were seen as mandatory in the achievement of security, together with consideration of continuing trustworthiness through all stages of the lifecycle of a *thing*.

The identified *Challenges* for protection of the IoT included architectures, standards, application security, privacy and trust, lifecycle, bootstrapping, network security, mobility, integration, trust and security models for *things*, together with consideration of principles such as the balance of centralized vs. distributed. These issues are being explored in an IETF draft, of which one of the speakers is co-author. A possible blueprint for a trust and security architecture was outlined and discussed, locating components within IoT from the point of view of trust and security.

### **Integration and discussions panel (J. Clarke, A. Sarma, R. Roman, M. Riguidel, F. Carrez)**

Fundamental questions that enquired about the nature and definition of *things* were raised, such as the hierarchical nature of things, how to record access (and who can have access to such records), recursion required and how information created by different things could interact.

The idea of fault tolerance and resilience in the IoT was introduced (“If hackers control part of the actual Internet, what will happen when the IoT arrives?”). Questions were asked about the creation of the security mechanisms (“do we need to integrate, adapt, or create security mechanisms in the IoT?”). There was wide agreement three approaches are necessary taking special care when adapting potentially causing unexpected knock on effects.

A stimulating (and controversial) assertion was made that the existence of an IoT with billions of elements raises major issues on governability that needs to be addressed, and that a more ambiguous world of intermittent connection might be necessary. However, it was agreed that this was indeed a major problem, and that the IoT will generate other new problems yet to be discovered and analyzed, and that benefits gained must outweigh those issues.

The first IoT International Forum will be held in Berlin on 22-23<sup>rd</sup> Nov. 2011 <http://www.iiot-i.eu/>

### **Links and Information**

[1] Full report and links [http://security.future-internet.eu/index.php?title=FIA\\_Budapest&action=edit](http://security.future-internet.eu/index.php?title=FIA_Budapest&action=edit)

## **This section contains the Questions & Answers during the sessions.**

Question: “In the definition of the IoT: does the requirement that you want to be able to uniquely identify *things* something that is really needed because if you look at sensor networks often it may not make sense to address individual sensors. For example, for temperature – you don’t need to identify individual sensors but groups of sensors instead?”

Answer: You may not need to identify the individual sensors, but from a management perspective, you may need to do so. We need to make a link to unique objects – only so that you can know what the data refers to (e.g. temperature). The *thing* is the item that is being monitored.

Question: “The definition is very restrictive in that it says that the *things* are available to everybody, and secondly assumes there will be one business model. For example, if we consider the ‘accessed by anybody’ (open Internet of Things vs. constrained Extranet of Things) part, we might limit the IoT to one single business model. Other companies might need something different”.

Answer: A common definition should exist to differentiate the IoT from other fields of research. There is a need to have a common definition and there are discussions about Intra-net of things and Extra-net of things. But the Internet should be more open – there’s a bigger concept behind it. Somehow it has to pay, and the only thing you can charge for is the data.

Question: “The business model does not convince me. We are not used to this kind of ‘pay for one-off pieces of data’ by the item in the Internet. (e.g. pay per article). The Internet of things should provide means for application developers to get revenue, not necessarily just for the data from the *thing*, which might be a dis-incentive for the development of applications by developers.”

Answer: We need a certain incentive for increasing the deployment of IoT technologies and development of new applications. Besides, the business model is based on the following question: ‘Are we willing to pay for information provided by the IoT?’ In fact, in the real world, we do pay, for example, through downloading apps, paying for the IT department by the slice, product sales and the selling of data.

Question: “You propose an architecture of the various Internet of Things. In proposing an architecture, it’s important that the architecture provides access to any objects in an interoperable way. Do you think that all systems should be built this way, so that they can all interoperate?”

Answer: To a certain extent (e.g. at the discovery service level), we should follow the same approach. Of course, we will have heterogeneity, but we need some common standards enabling interlinking of the different approaches such as common discovery services, semantic approaches, using information from different sources.

Question: “There was mention in the presentation about the use of linked data for the IoT, and whether the source of such data could be deemed trustworthy and reliable. What do you mean with the problem of ‘who provides the data?’”.

Answer: It is a challenge about data provenance and we need to know if the source of the data can be trusted.

Question: “You argued for a layer of sensors and a layer of applications including billing – the world is indeed a complex place. There will be sensors everywhere and a multitude of sources of IoT transactions (multiple initiators, etc.) and the notion of sensors we can always access is very good. But: do we really require customer billing for this or make this a main driver as

discussed in the presentation on business models? At least, we should consider the existence of an accounting and management component, which might be just everything we need instead of individual billing systems that could frighten off users who aren't accustomed to this type system. It raises questions: Whom are you billing? What about charging ISPs?"

Answer: It is true that accounting and management is important. However, existing accounting solutions may not be able to deal with the huge amount of possible 'billable' interactions in an Internet of Things. The ensuing discussion showed that this is still a contentious point, which requires further research.

**The following section contains the interventions wrapping up the session and final questions to the panellists in the closing session.**

**Amardeo Sarma, NEC.** "As we are in the phase of developing concepts and ideas for the IoT, the presentations raised quite a lot of views on the nature of things raising the question: "What are the *things* in the Internet of Things?". In the talks, we have heard *things* referred to as many possibilities from the IERC survey (sensor networks, RFID, M2M, etc.), real world objects (even trees and cows!) and identifiable end points. There are other issues related to the hierarchical nature of *things*, how to record access (and who can have access to such records), and how information created by different things could interact. This raises a need to identify things to different levels for example in the room that we are in and then the loudspeaker in the room. Based on this, a number of questions were put to the panellists:

1. Where we have identifiable things, e.g. hotel, then things within things, like the room, loudspeaker, do we need a recursive composition of *things* and should it be part of the architecture?
2. From the discussions on billing and the nature of how people use and pay for *things* nowadays almost for free, shouldn't we urgently address the business models from the very start?
3. regarding naming and addressing for IoT, this raises issues such as how to get bootstrapping, deployment and discovery?

**Responses from the panelists:**

Yes, for the IoT, it is definitely necessary to have recursions - eg. pallets with objects on them, that's recursive - and this has already been accomplished to a certain degree. There needs to be hierarchal identifiers with descriptions that are more complex (rather than single hierarchy) when dealing with devices in IoT. A mechanism is needed to define the scope of recursion to allow different layers of aggregation for the IoT and FI with multiple models to fit the hierarchy of devices. It was pointed out that we need to make sure not to mix the address and identifiers. There is room for intelligent clustering – an example of a truck carrying special loads was given.

Regarding the previous point on the definition of IoT, the speakers all agreed it is the usual situation where the definition is a hard one to find and there is a tendency to over dwell on this issue - but this should be less important with the primary focus being on the IoT Architecture (IoT-A) instead and defining the concepts within and below that. IoT-A results should be a step forward in this regard.

**Rodrigo Roman, University of Malaga** pointed out the importance of security and trust for the IoT to be successful and it necessitates a holistic point of view from the cradle to the grave and to see the different instances of the Internet of Things that are different. Mr. Roman introduced the idea of fault tolerance in the IoT ("If hackers control part of the actual Internet, what will happen when the IoT arrives?"), and questioned the panellists about the creation of the security mechanisms ("do we need to integrate, adapt, or create security mechanisms in the IoT?").

**Response from the panellists:**

All previous speakers agreed that all three approaches are necessary and this was also discussed at the IETF workshop<sup>1</sup> in Prague. However, the risks associated with ‘adapting’ were pointed out that could cause unexpected knock on effects elsewhere. A solution proposed would be to leave the interfaces open. The notion of **trust** in IoT is currently not clear and is a major challenge for the community. The observation was made that *things* have a lifetime, and they evolve over time (they are not static!) and there is a definitely a need for **fault tolerance** in IoT, and that it will be resilient to attacks.

Finally, **Michel Riguidel, Telecom Paris-Tech** brought some welcomed controversy to the session by declaring that the existence of a one single providential Internet of Things with billions of elements raises some major issues for him on trust, security and especially governability. In essence, Prof. Riguidel doesn’t agree with the concept that the IoT should be centrally governed/managed/administered since there are fundamental issues of personal freedom, online ‘liberties’ that we need to ensure are maintained, and he feels this cannot be accomplished by having a centralised IoT/FI governance model. Today, it is a closed world of hosts of billions of computers and the idea of having trillions of virtual, physical, static, nomadic objects raises thorny questions for Prof. Riguidel such as: Who will govern this? Where is the directory of this world? Who is going to manage the secrets?

Professor Riguidel raised the following questions:

- This leads to a double edged sword – do you want an Internet of Things that is connected all the time to everyone or one where things are only connected from time to time?
- What about personal freedoms? – especially not leading to a situation that is centrally controlled, monitored, watched?
- the tracking services of parcel providers are not questioned today, although they could have potential security and privacy implications for individuals. Will people keep these attitudes or become more conscious of their privacy in future?
- will devices really be uniquely identifiable? Prof. Riguidel asserts that maybe this is not realistic.
- there is a need to be more precise when talking about the IoT terminology. For example, what do we mean when we speak of IPv6 in FI? Do we refer to the *format* or the *protocol*? Prof. Riguidel argues that discussions in the IoT/FI community so far seem to be more about *format* than *protocol*, which can lead to a dangerous situation. This is a subtle point that deserves more attention especially at the edge of networks.

### **Response from the panellists:**

The panellists agreed that the IoT will generate new problems (which must be discovered and analyzed), and the benefits must outweigh those problems. We must clearly differentiate between the Internet of People and Internet of Things and there is also a differential between dumb things and intelligent things that must be made. Yes, today we are on one Internet and there are billions of devices and from the outside it looks like one Internet of Things, but on the inside there needs to be differentiated, federated sets of services and devices.

Regarding governance, all panellists also agreed that it is an important problem that must be tackled following the conceptual and definitions phases to ensure security and trust in the IoT. In fact, in the current Internet, this is only partially solved.

---

<sup>1</sup> <http://www.iot-i.eu/public/events/interconnecting-smart-objects-with-the-internet-workshop>