

Session II3. Internet of Things and the Future Internet, FIA Budapest, Wednesday 18th May 2011, 14:00 – 16:00.

ORGANISERS / CONTACT

Jim Clarke, Rodrigo Roman, Trevor Peirce, Antonio J. Jara, Antonio F. G. Skarmeta, Francois Carrez, and Alessandro Bassi.

BACKGROUND

The Internet of Things (IoT), which is one of the major topics in the Future Internet Week being addressed in Budapest, is becoming slowly but steadily one of the core elements of the Future Internet (FI). In fact, various architectures and approaches (e.g. using web services to connect directly “things” to the Internet) are being developed as of today. At this particular point, it is essential to discuss what are the IoT-specific aspects that the FI architecture has to take into account, in order to efficiently map the IoT architectures into an overall FI architecture.

OBJECTIVES / DESCRIPTION

The main goal of this session is to highlight various aspects of IoT architecture and how it should map to the FI. It is expected this mapping will lead to major challenges associated with scalability, manageability, addressing/identity, and robustness. In addition, the openness and ubiquity features of the FI will present different horizontal challenges to offer a suitable support for security, privacy and trust. Therefore, this session is focused on the presentation and discussion about the main challenges to be solved in a first step, in order to make feasible the direct inclusion of the Internet of Things in the FI supporting, in a safe and suitable way, the new generation of Internet services based on the Internet of things such as global health monitoring, smart grid or new concepts such as the Web of Things.

FORMAT OF THE SESSION

The session is divided in two main panels and final closing panel to highlight topics not adequately addressed, involving questions and interaction with the audience. The first panel presents real examples and specific details, requirements and design issues to make feasible the integration of the Internet of Things in the Future Internet. The second panel, picks up where the initial panel leaves off with a deeper analysis of the security, privacy and trust issues for the integration of the Internet of Things in the Future Internet, which is one of the most important challenges to be addressed in the current status.

Panel 1. IoT/FI architecture and integration:

- IoT Technologies Consolidation: Interoperability issues, moving towards all-IP networks, RFID (EPC) and IP integration, addressing issues, etc.
 - *What features and specifications need to be supported by the devices for the next generation of networks?*
 - *How to adapt the current solutions to the Future Internet of Things?*
 - *How to reach a suitable integration of the electronic devices, current solutions, and address the users and applications requirements in order to satisfy issues such as the scalability, power performance and costs in the Internet of Things-based deployments?*
- Protocols: Presentation of some of the crucial design issues from the requirements and constrains which are presented from the hardware level.
 - *How technologies and protocols deal with some of the challenges (e.g. mobility protocols)?*
- Services: Design issues and considerations for service deployment in real applications.
 - *Web of Things and Restful for the services based on Web?*
 - *How are being defined the business models and accountability of the services?*

- *Example of a real application such as e-Health or smart grid of the Internet of Things, and the design issues considered for them.*
Example of a real application such as e-Health or smart grid of the Internet of Things, and the design issues considered for them.
- *How could be applied the IoT for dissemination of the information?, could the ubiquity of the IoT be the next medium to reach the citizens?, how should be the policy and regulations of this in order respect user privacy and not to annoy with the excess of information and advertising.*

Panel 2. IoT/FI privacy, security & trust:

- Considerations for the Future Internet architecture for the privacy and security management in the Internet of Things.
 - *How clean state architectures for the Future Internet envision the IoT integration and the management of privacy and security?*
- Assuring a trusted, private, secure, fault-tolerant IoT infrastructure.
 - *How to achieve this goal, having in mind the heterogeneity of the IoT and other non-technological factors (e.g. EU policies)?*
 - *How to efficiently integrate the different security solutions with the FI architecture?*
 - *What fundamental limitations and IoT specific requirements must be considered?*
- How should the "gateways" and "border or edge routers" be involved in those communications.
 - *What tasks should be carried out by them?*
 - *How will it affect privacy when delegating the trust to the gateways?*
 - *What about the scalability when all the communications to an edge network based on e.g. 6LoWPAN need a pre-process and post-process from the Border Router?*
- Methods for validating security requirements against architectural solutions.
 - *How are considered solutions such as a "Security officer" role within IoT-A?*
- Impact of the security to other issues and challenges from the Internet of Things such as interoperability, scalability, discovery of things, accountability, and manageability.
 - *How affect/impact the security to these issues?*
- Policy related actions and new regulations addressing the new issues of the IoT
 - *Relationship between existing IoT-specific EU regulations and technological advances. Are IoT policies too far ahead of technology/research?*
 - *How could the EU make awareness to the citizens about the new security aspects, privacy issues and considerations for the new generation of communications based on the IoT.*
 - *Which regulations should be defined/refined in order to solve the mentioned security aspects?*

AGENDA

5 min	Presentation of the agenda and session objectives	Alessandro Bassi, IOT-A
40 min	IoT/FI architecture & integration panel: <ul style="list-style-type: none"> ● Topics to be addressed detailed above. ● Format: opening and presentations will last 25 minutes and immediate questions/discussions will last 15 minutes. 	Moderator and opening: Alessandro Bassi, IOT-A Panellists: Stephan Haller, SAP, Dieter Uckelmann, BIBA.
40 min	IoT/FI privacy, security & trust panel: <ul style="list-style-type: none"> ● Topics to be addressed detailed above. ● Format: opening and presentations will last 25 minutes and immediate questions/discussions will last 15 minutes. 	Moderator and opening: Trevor Peirce, IERC Panellists: Oscar Garcia, Philips Antonio Skarmeta, Univ. of Murcia
25 min	Closing panel: <ul style="list-style-type: none"> ● Summary of the sessions and fusion of the current status of the IoT and its integration in the Future Internet. ● General issues and not adequately addressed topics and discussions from the audience. ● Format: short interventions (2-3 minutes) on topics of coverage and questions for speakers and time for audience questions/discussions. 	Moderator: Jim Clarke, WIT Panellists: Amardeo Sarma, NEC Rodrigo Roman, Univ. of Malaga Michel Riguidel, ENST
10 min	Session conclusions and announcement of the IOT International Forum.	Francois Carrez, Univ of Surrey