www.enisa.europa.eu

Interview with ENISA Risk Management Expert, Barbara Daskala around the IoT/RFID Scenario Risk Assessment

ENISA Risk Management Expert, Barbara Daskala, is the editor of the IoT/RFID Scenario Risk Assessment report called "Flying 2.0, Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology".

First of all, how well known is this term "Internet of Things"?
This term has been mostly used so far within specialised communities, so you may say that it is not a term that the wider public is familiar with. However during the last years the term has slowly started to be used more frequently, also in conferences etc. You need also to understand that the there are other terms that are used interchangeably and denote more or less the same thing, and that's "pervasive computing", "ubiquitous environments", even "ambient intelligence". As discussions among stakeholders intensify, we see also new terms adopted as "Future Internet", which right now, at least for EU-related research, is almost an umbrella term, including " Internet of Things", "internet of services" etc. I guess the coining and use of the term can turn into a rather philosophical discussion, but what's more important here is to keep here is the main point behind this vision.

In the report you say that the "Internet of Things" (IoT) is a vision where all manufactured things can be network enabled, that is connected to each other via wireless or wired communication networks. Will this be the case you think?
We are definitely moving towards the direction that increasingly more everyday activities (communication, transactions etc.) are happening seamlessly, making things easier for people and enhancing the provision of services. It is important to note that this is a vision, and whether we reach it or not, or indeed whether it is going to materialise as we envisage it, depends on many different variables, technology is definitely one of them, but not the only one. We are all now in the position to influence this.

Who are the drivers and stakeholders of this technology?
There are many drivers and equally many stakeholders at the global level, which assume different roles. Generally speaking, main stakeholders are the industry, the EU Institutions (at the EU level) and other International Organisations (e.g. ITU), research institutes, laboratories and academia and of course governments. A main driver behind this vision is as I mentioned enhancing the provision of services, and as such facilitate and enhance citizens' lives; technologies are never developed just for the sake of it; this technology needs to be regarded as a key enabler.

Is legislation keeping up with the technology breakthroughs?
This was one of the major risks identified in the report, so the answer is no. Unfortunately, the legislation tends to lag behind technological advancements. It is important to be proactive though, and through studies like the one we did but even more focused, identify areas of considerations that legislation needs to address; again

this is a multi-stakeholder approach and cannot have a one-off solution either. On the other hand though, understandably legislation always takes time to be decided and implemented.

What are some of the technologies involved in IoT and apart from the air travel scenario, where can this technology be used?
RFID, location based services, wireless technology, biometrics, sensor-based networks are just some of the major technologies in the IoT vision; however, it is important to note that it is the convergence of all these technologies that makes such a vision possible. There are many discussions on the application of the Internet of Things and its technologies: e.g. in the supply-chain, in retail, in travel (as we also see in this air travel scenario). To summarize, it is a convergence of all the different technologies involved in the vision of IoT, where the users won't even understand which technology they are using.

There are apparent benefits with the IoT, but what are the concerns of this technology, but in the report you identified 18 major compound risks. Are there any of these that you would like to highlight?
It is very important to highlight the risks and challenges of how to implement the vision and how to enhance the service provision; hence our study. In the report, although there is no detailed analysis of the benefits, they have however been considered, and they are the major driver behind its existence: exactly because there are so many envisaged benefits of the new technologies, we need to proactively identify the major challenges that it may pose and try to address them appropriately.

There are many security risks that have to be addressed and which have to do with the technology itself and its implementation. And then there are other implications concerning privacy and data protection: the aggregated amount of data, and the increased possibility to link all this data, is a serious challenge since people might not be even aware of when and how their data is being shared and/or processed. One challenge is to ensure the citizens that their data is properly handled. For instance, companies might use people's data for other purposes than the ones they were initially collected for, also using profiling techniques. Surveillance is also another important consideration, since a limit needs to be drawn to the level of surveillance taking place to ensure national security and that, which results in violation of citizen's privacy rights. It may also have additional implications, such as social exclusion, for instance for people that are not that friendly with new technologies, who might be intimidated to use this kind of technology. This in turn might lead to people being excluded from the provision of services.

Is this up to the legislation to deal with?
I would say that legislation is only one way to deal with these issues, since it cannot and should not be the only way to deal with these issues. We don't want to over-legislate and over-regulate, since that might lead to the full benefits of the services not being available. This should be a mutli-stakeholder effort, where e.g. the EU institutions and the member states governments need to create an awareness of the risks and make sure that the companies are being ethical.

Are there any awareness raising campaigns around the IoT?
I don't think there has been any major awareness raising effort for the public as yet, especially since this is an emerging technology not yet fully deployed. At a certain point, we would need however awareness raising events highlighting the benefits of the technologies and the challenges posed; we would even need to look beyond awareness into educating the public on these issues. Once the IoT gets completely out of the lab and into our everyday chores, people would be definitely interested in knowing what this means for their lives.

Are people concerned that these new technologies might take over their jobs?
A specific analysis of these implications was outside the scope of our study, since as you see the focus is on the information security and privacy aspects. However, we could say that by all means people would be concerned, as it happens with the introduction of any new technology ever since the industrial revolution. It is also true that whenever you introduce new technologies, new jobs are created, that require new skills and expertise. It is an important issue, no, a crucial issue, for the governments and other decision makers, of how to handle the transition appropriately, and it requires a holistic approach, so as to ensure the well-being of the citizens, which at the end of the day is the paramount consideration.

What are the next steps when moving forward with the work of the IoT?
At the EU level, there are many EU funded R&D projects, looking at how to enhance the technologies, and studying also various implications, as our study did. There are many initiatives by many stakeholders, and a lot of debates currently are taking place as to how this vision would evolve, in which directions and what measures we would need to take to ensure its success. To this extent there are a lot of conferences at an international level taking place. Again, it is important to note that we need to make sure that all the stakeholders are taking part in the discussions, since its stakeholder has a very important role to fulfil.

For full report:
http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology

For press release see:
http://www.enisa.europa.eu/media/press-releases/flying-2.0-study-of-internet-of-things-rfid-in-air-travel

For further details, contact:
Ulf Bergström, Spokesman, ENISA press@enisa.europa.eu, Mobile: +30 6948 460143
Barbara Daskala, Risk Management Expert, RiskManagement@enisa.europa.eu