Flying 2.0? ENISA Launches Study on Future Challenges of Internet of Things/RFID in Air Travel

ENISA - European Network and Information Security Agency - April 12, 2010

BRUSSELS and HERAKLION, Greece, April 13, 2010 /PRNewswire/ -- Following up on European Commission communication on the IoT Action Plan for Europe, the EU's 'cyber security' Agency ENISA - The European Network and Information Security Agency, has analysed the risks associated with a future air travel scenario, enabled with "Internet of things", IoT / RFID technology. The report identifies major security risks, as well as privacy, social and legal implications and also makes concrete policy and research and legal recommendations.

IoT is a vision where all manufactured things are connected to each other via wireless or wired communication networks. The movement of travellers, airport staff, and luggage creates an increasing, continuous interaction between smart devices. It also implies sharing of significant amounts of sensitive information. Every day ca 28,000 flights occur in Europe, (i.e. ca 10 Mn/year), so the importance of air travel is easily understandable. The Executive Director of ENISA, Dr. Udo Helmbrecht, comments on the report;

"To fully realise the benefits of the Internet of Things, the challenges and risks that IoT implies must be identified and addressed in a proactive way. These risks do not always have to do with the technology per se but with the way we use it."

Three policy recommendations: 1. Rethink existing business structures and introduce new business models. Air transportation actors (e.g. airlines, airports, logistics, aviation security agencies, etc) should proactively stay alert for new business models. 2. User-friendliness and inclusiveness of devices, processes and procedures - we need to be inclusive. 3. Develop and adopt policies for data management and protection

Five research recommendations: 1. Data protection and privacy. 2. Usability. 3. Multi-modal person authentication, e.g. biometric procedures. 4. Proposing standards of light cryptography protocols, and 5. Managing trust as a central consideration: an enterprise should understand its own trust framework.

Three legal recommendations: 1. Support for users, e.g. for data subjects to better exercise their rights. 2. Placing a high value on information and data. 3. Harmonisation of data collection by airport shops and efforts to raise awareness among travellers of the collection and processing of data.

Three recommendations are given specifically to the European Commission: 1. Enforcement and application guidelines for the European regulatory framework. 2. Alignment of research with both
industrial and societal needs, e.g. ethical limits research. 3. Need for security and privacy impact assessment and trials of new technologies before deployment.


(Due to the length of this URL, it may be necessary to copy and paste this hyperlink into your Internet browser's URL address field. Remove the space if one exists.)