Innovation through research

Dr. Udo Helmbrecht, Executive Director, ENISA

ISMS Forum, Madrid 25 May 2010

Who are we?

- The European Network & Information Security Agency (ENISA) was formed in 2004.
- The Agency is a *Centre of Expertise* that supports the Commission and the EU Member States in the area of information security.
- We facilitate the exchange of information between EU institutions, the public sector and the private sector.

Activities

- The Agency's principal activities are as follows:
  - Advising and assisting the Commission and the Member States on information security.
  - Collecting and analysing data on security practices in Europe and emerging risks.
  - Promoting risk assessment and risk management methods.
  - Awareness-raising and co-operation between different actors in the information security field.

Focus

- ENISA assists Member States and the Commission in global issues that affect the European Community as a whole.
- This is an advisory role and the focus is prevention and preparedness.
- ENISA does NOT have any operational responsibilities either within the EU institutional framework or with respect to Member States.
- ENISA has no special role in the security process protecting EU institutions.

ENISA Research related activities

Previous work (examples)

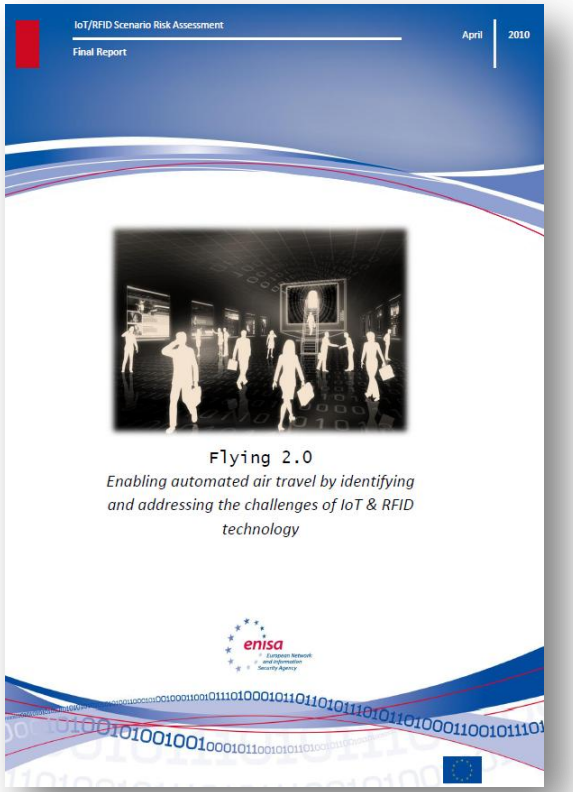
- ★"PROCENT"
- ★"Flying 2.0"
- ★Cloud computing

PROCENT

- The five research areas identified are:
  - cloud computing
  - real-time detection and diagnosis systems
  - future wireless networks
  - sensor networks
  - supply chain integrity

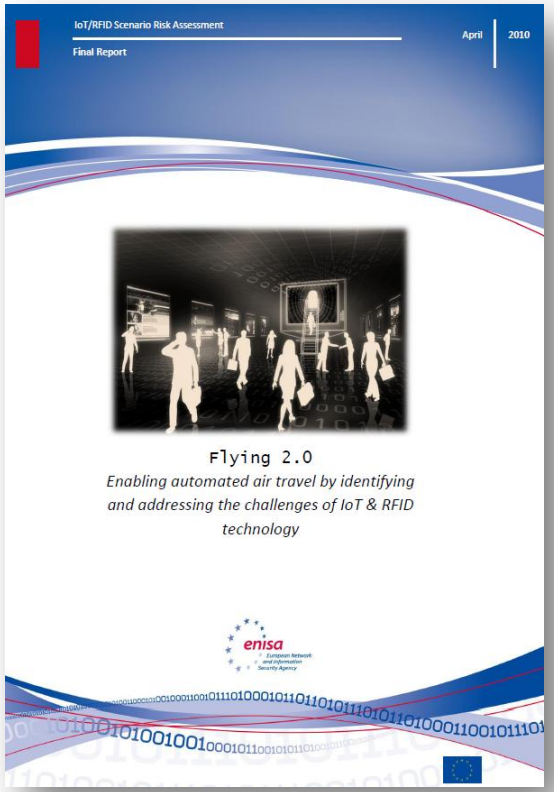
Flying 2.0

- Research recommendations
  - It is recommended to carry out research to examine the issues in relation to "Internet of Things" deployments and to further extend security and privacy solutions. Examples:
- Usability
  - It is recommended to investigate the issues related to usability of security and privacy technologies, human-device interfaces and assisted privacy policy (consent) specification and management.



Flying 2.0 (contd.)

- Managing trust
  - an enterprise should identify and understand its own trust framework in order to be able to deal with the IoT challenges.
- Multi-modal person authentication
  - It is recommended to further investigate and develop biometric procedures for person authentication.
- Proposing standards of light cryptography protocols
  - It is recommended to set up light cryptography standards and give some time to the scientific community to test them before wide implementation.



Cloud computing (2009)

- Research recommendations
  - The following are the categories we have considered with a few examples of specific areas from the full list:
- BUILDING TRUST IN THE CLOUD
  - Effects of different forms of breach reporting on security
  - End-to-end data confidentiality in the cloud and beyond
  - Higher assurance clouds, virtual private clouds etc.
- DATA PROTECTION IN LARGE SCALE CROSS-ORGANIZATIONAL SYSTEMS
  - Forensics and evidence gathering mechanisms.
  - Incident handling - monitoring and traceability
  - International differences in relevant regulations including data protection and privacy
- LARGE SCALE COMPUTER SYSTEMS ENGINEERING
  - Resource isolation mechanisms - data, processing, memory, logs etc
  - Interoperability between cloud providers
  - Resilience of cloud computing. How can cloud improve resilience?

Many thanks for your kind attention

Questions?