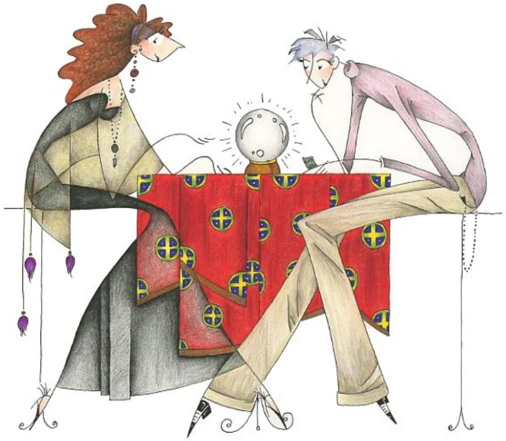
Looking through the crystal ball: *Identifying future security, privacy and social risks in a prospective IoT scenario*



SecIoT 2010

29th November 2010, Tokyo

Barbara Daskala, CISSP, CISA, ENISA

James Clarke, Waterford Institute of Technology, Ireland

Dennis K. Nilsson, Swedish Institute of Computer Science, Sweden

Why a ‘crystal ball’?

- IoT is a prospective vision
- Considering a possible future IoT scenario on air travel [ENISA study]
- Using a risk assessment approach to identify potential risks
- Putting things in context*: Covered many different aspects!*

ENISA ‘Flying 2.0’ Study

- **EC Communication “*Internet of Things – An Action Plan for Europe*”**

- **Main Objective**: identify and explore risks in a future air travel scenario, of emerging and future technologies and applications (IoT/ RFID, LBS…)

- Three different scenarios / three actors

ENISA Study WG Members

- **Alessandro Bassi**, Hitachi Europe SAS, France
- **Jim Clarke**, Researcher, Waterford Institute of Technology, Ireland
- **France Charles de Couessin**, Executive Partner, ID Partners, France
- **Sotiris Ioannidis**, Associate Researcher, Institute of Computer Science, Foundation for Research and Technology (FORTH), Greece
- **Eleni Kosta**, Legal Researcher, K.U.Leuven - Interdisciplinary Centre for Law & ICT (ICRI), Belgium
- **Paul McCarthy**, Research Fellow, Lancaster University, UK
- **Huang Ming-Yuh**, Program Manager, Strategic Information Assurance, The Boeing Company, US
- **Eurico Neves**, CEO, INOVA+ Serviços de Consultadoria em Inovação Tecnológica SA, Portugal
- **Dennis Nilsson**, Consultant at Syncron Japan KK, Tokyo, Japan
- **Milan Petkovic**, Philips Research, The Netherlands
- **Pawel Rotter**, AGH University of Science and Technology in Krakow, Automatics Department, Poland
- **Markus Tiemann**, Human Factors and Cabin/Cargo Operations, AIRBUS Operations, Germany
- **David Wright**, Managing Partner, Trilateral Research & Consulting LLP, UK

The '*Akira*' scenario

- **When**: *2015* - 5 years into the future
- **Who**: Akira, 20 year-old, a Japanese scholarship student
- **Where**: airport (London to Japan), on the way to the airport, on the aircraft, arrival
- **What**: Use of smart technologies to perform the various steps of air travel

The major phases in the scenario

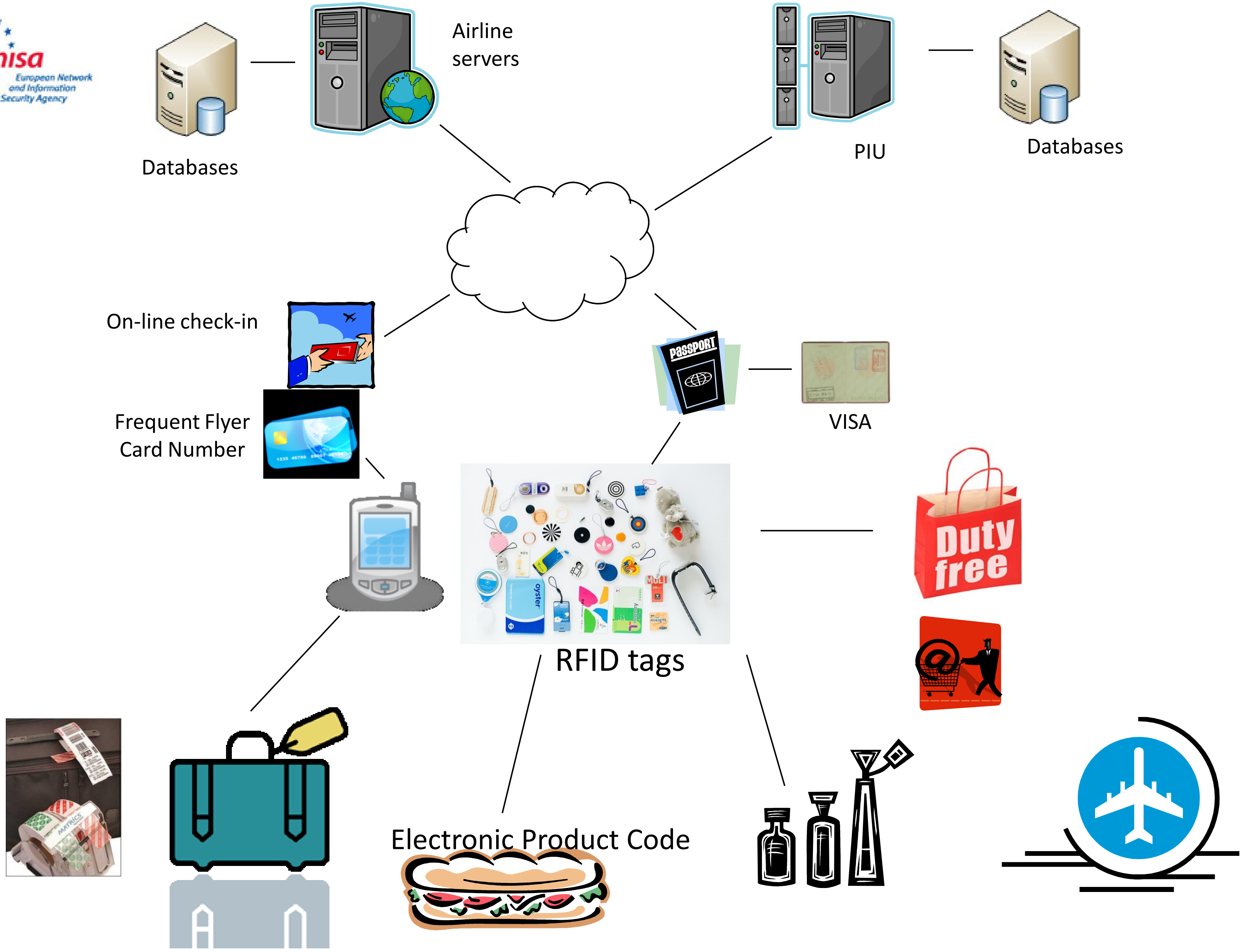
- **Getting to the airport –** the Tube, London, RFID enabled card
- **Airport check-in –** RFID-enabled frequent traveler card , fingerprint check
- **Security & border access controls**
- **Waiting to board –** Social networking [JP-Professionals-unite.com]…
- **Boarding –** seamless
- **In flight –** Internet in the air [ad-hoc network], Creative Commons
- **Arrival and transfer –** Frequent flyer card contains luggage tags

The major phases in the scenario (cont'd)

- **Boarding –** seamless, smart boarding process based on verifying 2D barcodes as well as biometrically authenticating passengers

- **In flight –** Internet in the air

- **Arrival and transfer –** Personal electronic devices and airport infrastructure guide passengers through immigration control, luggage claim, and onwards to bus, train or rental car



Airline servers

Databases

PIU

Databases

On-line check-in

Frequent Flyer Card Number

VISA

RFID tags

Electronic Product Code

The risk assessment in brief

- Methodology based on ISO/IEC 27005:2008
- Identify and valuate assets (values, rights, systems, services…): ***composite asset*** [data & physical device]
- Identify and assess vulnerabilities (of assets) and threats
- Identify and assess major risks in the scenario
- Make recommendations

What are we trying to protect? – *The assets*

INTANGIBLE

- Automated reservation, checking and boarding procedure
- Electronic visa issuing process
- Luggage and goods handling
- Automated traffic management

TANGIBLE

- Passports and National ID cards
- Mobile ‘smart’ devices
- Health monitoring devices
- Travel documents (paper)
- RFID & barcode readers
- Credit Cards/Debit card/Payment cards/'e-wallet'
- Other RFID cards
- Scanners & detectors
- Networks
- State databases
- Commercial and other databases
- Temporary handset airport guides
- Luggage and goods
- Check-in infrastructure
- Airport facilities

Identifying major risk areas…

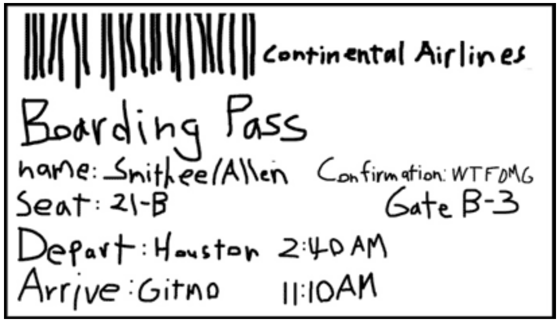
Technical

- High dependency on technology...
- Overall computing network infrastructure failure ➡ *Severe service interruption and unavailability*
- Realisation of malicious attacks to compromise systems (e.g. social networking, DoS attacks, cloning of RFID tags, jamming, blocking, side channel attack)
- Electronic ID failures: identity theft…
- Failure of vehicles and ground transportation infrastructure

⬇

traffic jams, accidents etc.

Identifying major risk areas… (cont’d)



Continental Airlines

Boarding Pass

name: Snithee/Allen Confirmation: WTFDMG

Seat: 21-B Gate B-3

Depart: Houston 2:40 AM

Arrive: Gitmo 11:10AM

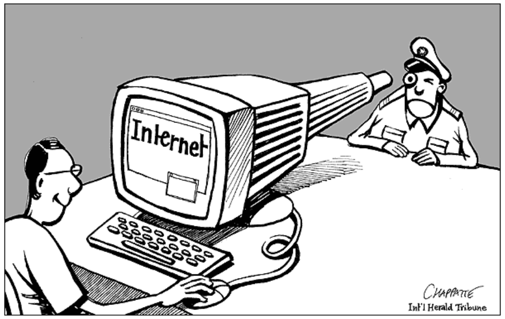
Policy & organizational

- Reservation, check-in and boarding procedures rendered unavailable
- Security screening failure (e.g. scanners malfunction, failure of procedures etc.)
- Interoperability issues across countries
- Cannot issue/control electronic visas
- Inability to travel: loss of paper documents, other delays / failures, check-in / passenger identification
- Procedures / instructions , devices complex to use → not followed

Identifying major risk areas… (cont’d)

Social (including privacy)

- Function creep / repurposing of data
- Loss of privacy
- Social sorting and social exclusion
- Increased surveillance
- Low user acceptance, user frustration



Identifying major risks… (cont’d)

Legal

- Lack of common or harmonized data protection legislation
- ‘Legal vacuum’ – Legislation lagging behind technological advancements
- Non-compliance with the data protection legislation

NOTE

Various risks are highly interconnected!

Distinction between security, privacy risks not always very clear!

And now what?

Addressing the risks requires considering many aspects…

POLICY

- Rethink existing business structures and introduce new business models
- User-friendliness of devices and procedures, include rather than exclude!

RESEARCH

- Data protection and privacy
- Usability
- Managing trust
- Multi-modal person authentication
- Proposing standards of light cryptography protocols

Recommendations (cont'd)

LEGAL

- Reevaluate and update data protection legislation
- Harmonisation of data collection

FOR EUROPEAN COMMISSION

- Enforcement and application of the European regulatory framework
- Alignment of research with industrial and societal needs
- promoting participation of industry, and in particular SMEs in research activities as FP7
- Ethical limits research
- Need for impact assessment and trials of new technologies before deployment

Some conclusions...

YES!

IoT is a promising vision and may solve many problems!

BUT...

There are **important risks** posed that need to be addressed

SO we need to...

- be proactive

- weave security & privacy into IoT

- work together!

[existing EC initiatives on Privacy Impact Assessment framework of RFID applications and IoT Expert group and]

Thank you!

ありがとうございました!

✉ barbara.daskala@enisa.europa.eu

For the ENISA report, visit:
http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables