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

Barbara Daskala
ENISA (European Network and Information Security Agency),
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13 Heraklion, Greece
<Barbara.Daskala@enisa.europa.eu>

Paper – Invited Talk

Abstract

The Internet of Things (IoT) vision offers new exciting ways to perform various everyday activities. However, in such a vision where "everything" is connected to "everything" to provide seamless and improved service, several challenges arise especially in respect of trust, privacy and security. In this paper, we have considered a prospective scenario in air travel where IoT is an enabler for a plethora of improvements, novel services and business opportunities. Moreover, based on a recent study by the European, Network and Information Security Agency (ENISA), we follow its risk assessment exercise and consider its results regarding the major vulnerabilities and threats identified in the air travel scenario; we further discuss what we consider to be the general challenges for future IoT applications extending beyond the air travel scenario. Additionally, we provide a set of recommendations to be considered by various stakeholders when designing and deploying future IoT scenarios. We believe that IoT is a key enabler for a wide range of services and applications; however, the risks entailed in such a vision must be thoroughly investigated and carefully considered during design and implementation and prior to deploying any IoT solutions.

1. INTRODUCTION

The Internet of Things (IoT), sometimes referred to as ubiquitous networking or pervasive computing environment, is a vision where all manufactured things can be network enabled, that is connected to each other via wireless or wired communication networks. It links the objects of the real world with the virtual world, thus enabling anytime, anyplace connectivity for anything and for anyone [1].

The excitement over this undoubtedly promising future of technology is being somewhat subdued by the discussions on the potential challenges and risks it entails associated with IoT usage for people. However, there is clear evidence that there is no holding back from the various involved stakeholder's determination to study and carry out the necessary research on these technologies that could transform the way we live our lives. For example, the Conferences "On RFID: The Next Step to the Internet of Things" held in Lisbon during the Portuguese Presidency on 15-16th November 2007, and subsequently the conference on "The Internet of Things Europe 2009: Emerging Technologies for the Future" in May 2009 concluded with a consensus for Europe to analyse, assess and develop common strategies for optimising the shift of RFID technology into the "Internet of Things", whilst safeguarding sensitive information and protecting the privacy of individuals. Moreover, with the advancement of ICT technologies, the number of different ordinary devices that increased their capabilities well beyond their original purpose is dramatically rising. These smart devices, which are the bricks needed to realize an "Internet of Things" (IoT) are poised to create significant impact on many areas of our lives. Clearly, we are currently only experiencing one part of initial phases of Internet of Things technologies but what will it really be like in the future? What would Internet of Things mean for our daily lives and existence? In order to visualise such a future life, we have considered a prospective IoT scenario in air travel, taken from the European Network and Information Security Agency (ENISA)'s technical report [2], to act us a basis for our risk assessment.

Given that we are already seeing the introduction and use of smart technologies and applications in air travel (e.g., RFID-enabled passports, electronic boarding

passes sent using SMS and displayed on cell phones), we consider this as a representative, realistic yet emerging, showcase scenario within which we can identify and highlight important risks and challenges posed by IoT technologies.

We realise that there are clearly benefits of IoT: various airlines have already improved significantly their operational efficiency by utilising Internet check-in, electronic boarding passes, RFID-enabled luggage handling, as well as e-enabled airport check-in and boarding. The adoption and deployment of smart devices is bound to improve their efficiency even further. Similarly, border control and airport security agencies can make use of these technologies to achieve a more accurate and efficient screening process. From the passengers' perspective, improved convenience comes from reducing or even eliminating the need to carry and manage various pieces of documents, certificates and other sensitive assets. While IoT will inevitably play a major role in improving future air transportation, as it will in many other areas as well, there are critical issues to be identified and considered in depth.

This paper is based on recent work performed by ENISA on the subject, and the technical report it produced as a result [2]. ENISA's study considered three different scenarios of three travelers from which a comprehensive risk assessment based on the ISO/IEC 27005 standard was performed identifying assets, vulnerabilities, threats and finally the risks posed in such a scenario; furthermore, the report identified some recommendations. Our paper is based on this work with the objective to highlight the need to be proactive and perform such risk assessments for other possible IoT environments. Additionally, we would like to emphasize what seem to be the major risks of such a vision (not only for the air travel scenario), as most of the collective risks identified in this study are valid for other IoT implementations. In this context, we have selected one scenario from the three included in ENISA's technical report, to provide the basis for our analysis in this paper.

The main contributions of this paper are as follows.

- We explore and present a future neutral IoT scenario as a showcase of the potential of an IoT vision, and which can provide the base for an appropriate analysis for IoT, as was performed in the context of the ENISA study [2].
- We present a comprehensive risk assessment approach of such a scenario, where assets, vulnerabilities and threats are appropriately identified; thereby highlighting the importance of a proactive approach in understanding the risks entailed. Based on this risk analysis of the air travel scenario, we project and discuss these risks and challenges in a generic context applicable to other IoT deployments.
- Finally, we provide some general recommendations and policy options applicable for various stakeholders and in the majority of IoT environments.

The remainder of this paper is structured accordingly. In Section II, we present a prospective scenario for future air travel taken from the ENISA report. Next, in Section III, we briefly give an overview of the methodological approach taken for the risk assessment by ENISA; it also provides an overview of the assets, vulnerabilities and threats identified in the air travel scenario. Section IV describes in detail risks identified for future IoT scenarios, not only applicable to the air travel scenario. In Section V, we provide a set of general recommendations for countering these risks. Finally, Section VI concludes the paper.

2. A PROSPECTIVE SCENARIO

The scenario is based on one of the scenarios from the ENISA technical report [2]. It differs from other prospective scenarios built in the sense that it presents a positive to neutral image of the future applications. This is done on purpose since this scenario forms the basis upon which potential risks are identified later in the risk assessment. An overview of the IoT air travel scenario is depicted in Fig. 1.

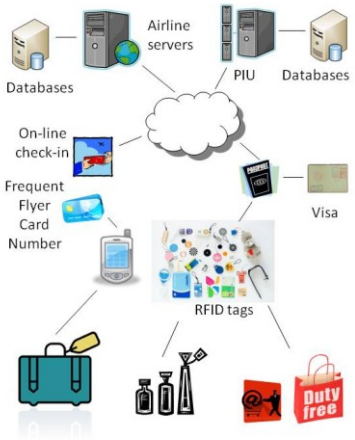

Fig. 1. IoT air travel scenario where various devices/cards/procedures are interconnected.

London 2015. Akira, a 20-year-old Japanese architecture student, is returning to Tokyo, with Nihon Airlines, after studying on a scholarship at the University of London. Before he left Tokyo a year ago, he received a one-year visa for the time he was to spend in the UK. As a Japanese citizen, Akira benefits from the registered traveler program agreed between the European Union

and several countries, one of which is Japan. Akira has filled out, 24 hours in advance, his PNR form online which was then reconciled with his Global Entry registration data by the UK Home Office in London. The latter positively matches the PNR against his Global Entry registration data.

Still online, Akira visits the duty-free section on the airline's website and buys a few gifts for his parents. The airline attaches RFID tags to the items indicating that Akira is the rightful owner. The items will be loaded onto the correct airplane based on his boarding pass information and given to Akira when he is in mid-air.

Akira takes the Underground to Heathrow. He pays for the journey using his RFID-embedded Oyster card. Transport for London (TfL) maintains a record of Akira's payments as well as all the travels he has made using the card.

As Akira has not checked in yet, he approaches a kiosk in the departure terminal of the airport to check in. He owns a smart phone device, but since it is not 100 per cent compatible yet with the European check-in procedures, he prefers to use his Nihon Airlines RFID frequent-flyer card. He presents his RFID-tagged frequent flyer card to one of the designated RFID readers. He is also asked to put one of his fingers on the scanner, which compares it with fingerprint features stored on the frequent flyer card (which prevents Akira's frequent flyer card, and consequently the boarding pass stored on it, from being used by another person). The reader sends information about the flight, seat number, and the duty-free goods that he bought online etc. to the frequent flyer card. Now Akira can use his card as a boarding pass. When he presents his card to the reader, which is linked to the airline's departure control system, it confirms that he is indeed booked on the flight to Narita. At the same time, it updates the Passenger Information Unit (PIU) at the Home Office, which delivers an electronic travel authorisation (ETA), based on the processing of his PNR. He would not be issued an ETA if he had overstayed his visa period. This check-in procedure allows Akira to enter the restricted area.

At the self-check-in kiosk, the machine also adds Akira's flight details to the RFID tag embedded in his suitcase. The luggage tag receipt is then stored on his frequent flyer card. Akira can then drop off his suitcase at the nearest baggage drop. Akira puts the luggage on a conveyor belt, which dispatches it to the Tokyo flight containers for his flight.

He then proceeds to the restricted zone, which he enters by presenting his frequent flyer card to an RFID reader and pressing a finger against a scanner which confirms that the card containing his boarding pass belongs to him.

As he is leaving the Schengen area, he is directed to an automated passport/immigration control. The combined biometric data from both his visa and passport are checked to verify that he is the rightful owner and that he has not overstayed his time in Europe.

After passing the security check, he proceeds to his gate. He is registered on a Japanese professional network site (JP-professionals-unite.com) and is interested in making new connections with architects and interior designers, since he will be looking for a job in Japan. At the boarding gate, the application on his smart phone detects someone from Tokyo Architects Ltd waiting to board the same plane. Akira sends a message, which the other accepts; they agree to reveal their physical positions and soon they are chatting face to face.

On board and in the air, Akira turns on his notebook and soon forms a peer-to-peer ad-hoc network with 15 other passengers who share interests in travel to exotic places. Akira also connects to the Nihon Airline's flight entertainment system's free movie section and browses the movies but cannot find anything that he likes. However, he does find a couple of interesting documentary films, published under Creative Commons, about travels to South America which a fellow passenger shares on his video server. Akira spends some enjoyable hours viewing these. Akira reciprocates with some of the content and services on his notebook.

Akira also uses his notebook to select a Japanese dinner from the Nihon Airlines in-flight service menu website. One of the in-flight attendants brings Akira the duty-free items he had previously purchased via the airline's website. A match is made between the RFID tags on Akira's boarding pass and on the tagged items. As an afterthought, he connects to the in-flight duty free shopping menu from his notebook and decides to buy a heavily discounted Swiss watch for his girlfriend.

Akira arrives at Narita airport and proceeds to the luggage reclaim, where an automated system consisting of a number of stations returns all pieces of luggage exactly to their owners upon request. Akira approaches such a station and presents to a reader his frequent flyer card, which contains his luggage tags receipt. Within a few seconds, the system automatically moves his suitcases to the appropriate reclaim station, where Akira collects them.

As he does so, he receives a message from a well-established Japanese online dating service, to which Akira had been a subscriber and which is integrated with the LBS service of Narita airport:

"Dear Akira-san, welcome back. We hope you had a good journey. It is our greatest pleasure to offer you this opportunity to meet Sakura-san, a young lady of exceptionally fine matching attributes based on your "Hazukashi Nain" (Shy Not) social network profile. Sakura-san is not far from your current physical location and is willing to communicate with you. Please push this button for an instant audio/video connection."

- *But Akira has a girlfriend now and no longer wishes to receive such invitations. He wisely clicks on the "ignore" button and moves on towards the exit of Narita airport.*

3. THE ENISA STUDY AND TECHNICAL REPORT: BRIEF OVERVIEW

In this section, we will briefly give an overview of the ENISA report [2]. The risks and recommendations presented in Sections IV and V are based on the analysis performed in the ENISA study.

A. Methodology

The methodological approach used in the ENISA technical report to identify and assess emerging and future risks was based on the standard ISO/IEC 27005:2008 Information technology Security techniques Information Security Risk Management [3]. The following major steps were performed in the process of assessing the emerging and future risks:

- Assets identification and valuation
- Vulnerabilities identification and assessment
- Threats identification and assessment
- Identification of final risks

1) Identification and valuation of assets: In this step, the major assets are identified and their value is estimated. For the purposes of our analysis, asset identification was performed at the composite asset level, meaning that personal and other type of data was identified as part of a physical asset (e.g., a smart device, a health monitoring device, or a database) and not as a separate asset. As such, the estimation of the value of the physical asset considered also the value of the data that resides on this asset. In order to estimate the asset value, the impact of loss of confidentiality, integrity and availability is considered for each asset for a list of areas; for the purposes of this study the following areas have been identified:

- *Health / Life:* Refers to the physical and psychological condition of an individual; his/her physical and psychological well-being and absence of disease.
- *Time:* Refers to the time needed to get to the airport, check-in, clear security controls and board the aircraft.
- *Human rights and social values:* Includes privacy, autonomy, non-discrimination, dignity, social inclusion, trusted human relationships, etc.
- *Mobility of individuals:* Refers to the ability and potential of people to move across countries.
- *Financial / economic factors:* Includes costs for airlines, airports, companies and individuals.
- *Comfort, convenience and ease of access:* Refers to the extent to which services are provided and procedures followed without difficulties.
- *Interoperability:* Refers to the interoperability between networks, sensors, devices, organisations, passengers and users. An IoT-like network will depend on a high level of interoperability between all of the different contexts and situations in which devices will need to communicate.
- *Trust:* Is essential in all aspects of the scenario. Passengers must trust the information on their devices. Operators must trust personal data provided, and information provided to them by other operators. Trust is also needed in the automated procedures by airlines and airport operators. And border authorities must likewise trust in the systems to perform.
- *Business activities:* Includes all those activities performed by product vendors and service providers to generate revenues and earnings.

2) Identification and assessment of vulnerabilities: The purpose of this stage is to identify and assess vulnerabilities of the assets. A vulnerability refers to an aspect of a system/process (the assets) that can be exploited for purposes other than those originally intended. Weaknesses, security holes, or implementation flaws within a system that are likely to be threatened are examples of vulnerabilities. These vulnerabilities are independent of any particular threat instance or attack.

3) Identification and assessment of threats: This stage involves the identification and assessment of possible threats that could exploit the vulnerabilities of the assets identified. It should be noted that threats exist regardless of the vulnerabilities, and there are two major categories of threats to be considered: man-made and natural threats, namely threats due to humans (either accidentally or intentionally) and threats due to natural events (e.g., adverse weather conditions).

4) Risk identification and assessment: Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets [3]. Thus, the final risk and its value are a function of the three elements, namely:

Risk = f(Asset, Vulnerability, Threat)

A selection of assets, vulnerabilities, threats and risks are briefly described in the following section.

B. Assets

The assets provide the basis for the identification of the vulnerabilities, threats and finally risks. They can be tangible or intangible as well as be owned by various stakeholders such as passengers, states, airlines, or airport shops. The value of the assets is different for different entities and for different stages. For example, passport and ID card are extremely important for Akira, because without them he cannot travel. On the other hand, his passport and ID card are not that pertinent for airport shops. Similarly, boarding passes are more important prior to boarding than afterwards. The most important assets identified in this scenario are summarized below.

1) Automated reservation, checking-in and boarding procedures: the business processes underlying Akira's flight bookings, checking in, security control and boarding.

2) Passport and national ID cards: may be owned by state agencies issuing these IDs and by the citizens, these are the new generation IoT smart IDs with embedded RFID, digital photos, and biometric information (e.g., fingerprints and iris patterns).

3) Mobile "smart" device: Smart mobile personal devices owned by the passengers, such as cell phones and PDAs, will play a major part in the automation of future air transportation processes. The devices may store personal and location data.

4) RFID tag, RFID reader and barcode reader: An RFID tag can be on a card or imprinted on papers (e.g., boarding passes or luggage tags). Readers are typically owned by establishments such as airlines, airports or airport shops to authenticate boarding passes in performing business transactions or detecting customer browsing behaviours.

5) Credit cards, debit cards, payment cards, e-wallets: Owned by the passengers or the issuing institutions, these cards may be with or without embedded RFID, and they are used to perform transactions at various locations (e.g., check-in counters, airport shops, online purchase via smart devices).

6) State databases: State databases contain data on passengers, including information originally created by states (e.g., in passports or visas) or later collected by the states during the air travel process (e.g., border entry/exit, citizen location information, or citizen travel patterns).

7) Commercial and other databases: These databases contain passenger data held by businesses and entities other than state agencies. Many business functions such as market analysis or consumer pattern discovery drive the creation and collection of these potentially privacy-sensitive data.

C. Vulnerabilities

In this section, we present an indicative list of vulnerabilities identified in the ENISA study, accompanied with a short description. As mentioned in the methodology section above, the vulnerabilities are identified per asset, so each asset identified above may have one or more of the vulnerabilities presented below.

1) Inappropriate design of procedures: This vulnerability could be due to lack of accountability, high complexity of procedures, assigning extensive responsibilities to end-users (in critical parts of the procedures).

2) Excessive dependency on IT systems, network and external infrastructure: An excessive dependency arises when one relies on IT systems. It is a sort of "mug's game" in the sense that virtually every system will fail to a lesser or greater extent at some point or other.

3) Flawed/insufficient design and/or capacity of devices and systems: Poorly designed devices or systems may create a vulnerability, whereby they are not sufficiently robust or resilient to withstand attacks by cyber attackers or they may not do what is expected of them, especially at critical times.

4) Lack of sufficiently skilled and/or trained personnel [airport, airline]: It has often been said that the weakest link in any system is human. If personnel are inadequately trained, they become a vulnerability. They need to be trained adequately to detect and understand security threats and what to do in the event of a system malfunction.

5) Lack of respect of the data minimisation and proportionality principles: The data collected and processed shall be adequate, relevant and not excessive in relation to the purposes they are collected. An example of such lack of respect of the data minimisation and proportionality principles could be described as the case when an LBS system collects not only the information absolutely needed for the provision of the service, but it also stores excessive information. The need-to-know principle is not enforced by any means.

6) Inadequate security measures of data storage (e.g., inadequate encryption measures): For instance, for RFID and con-tactless smart cards, due to limited resources, manufacturers often apply light cryptography and proprietary cryptographic methods. These methods may rely on proprietary secrets and may not provide an adequate level of security.

7) Data linkability: Different databases or data stored at different locations serving different purposes could be

linked, thus enabling greater data matching, data mining, profiling, data aggregation or social sorting [9]. Key question here is who is doing the linking and why; it could be for security reasons (locating and apprehending terrorists before they fly), but it could also be for commercial exploitation by airlines, vendors, and service providers operating in the airport as well as by evil-doers seeking to undermine air travel, airport systems or engaged in spoofing, phishing, spamming.

8) Insufficient protection of wireless networks and communication (weak or no encryption): Due to limited resources, RFID tags often use light, proprietary cryptography, which in some cases is not sufficient. Identifiers of tags which are sent in the beginning of communication are not encrypted at all (as a part of the anti-collision protocol) and they may be used, e.g., for tracking of tags and people.

9) Lack of respect of the legitimacy of data processing, e.g., consent: The processing of personal data is supposed to be legitimate. However, some data controllers and data processors may not have obtained the informed consent of data subjects.

10) Lack of data correction mechanisms (as normally data subjects do not have access to the databases): Many entities are collecting personal data, but rather fewer of them have procedures in place enabling individuals (data subjects) to see what data they have about them. Procedures for correcting incorrect data may not exist or may be cumbersome and bureaucratic.

11) Inherent features (size, material etc.): easy to lose, to be stolen and/or copied (especially for RFID tags): Inherent vulnerability of cards and devices (passports, RFID tags, etc.); they are small in size, and they are easy to lose, be stolen and/or copied.

D. Threats

Below you find a list of some indicative threats identified in the ENISA study, and which pertain to the scenario presented above. Please note that the threats exist regardless of the vulnerabilities mentioned above. Each threat may exploit one or more of the vulnerabilities and result in the final risk.

1) Denial of service attack / flood / buffer overflow: A denial of service (DoS) attack is sabotage, aimed at disrupting a service for fun or to achieve political or malicious goals. A DoS attack could constitute a buffer overflow attack or flooding.

2) Spoofing of credentials / bypass authentication: This threat is a stepping stone to achieve the next stage of sabotage or penetration. For example, cloning of credentials or RFID tags could be used to gain unauthorized access.

3) Large-scale and/or inappropriate data mining and/or surveillance: The ease with which data can be collected, aggregated and mined, coupled with the motivation of large financial incentives make this a widespread threat. Both airports and governments may also have an interest in analysing data, preventing terrorist-related incidents, and developing more targeted advertising.

4) Man-in-the-middle attack: This is one of the most common attack methods, especially for information collection. However, such attacks on RFID and smart cards do not occur very often in practice today. Man-in-the-middle (or relay) attacks for contactless smart card has been theoretically analysed by Kfir and Wool [4].

5) Unauthorised access to / deletion / modification of devices / data: These attacks refer to unauthorized access to data stored on RFID, smart cards (especially contactless) and personal devices. Also databases can be subject to attacks through the network, as well as data can be illegally accessed and modified by unauthorized personnel.

6) Side channel attack: Smart cards or RFID tags may be subject to side channel attacks based on information gained from the physical implementation of a cryptosystem, like variations of power consumption, time of computations or electromagnetic field [5]. It is often combined with other cryptanalysis methods.

7) Jamming: Jamming is malicious interference of a radio transmission. It can result in denial of service and forcing a system to use fallback procedures. Large-scale jamming requires extensive equipment setup and exposure of the transmission source. It is not commonly practised unless with a clear and critical agenda.

8) Fake / rogue RFID readers / scanning of RFID reader and / or tag: RFID Tags can be read by any RFID reader. Therefore, rogue RFID readers can scan for RFID and be used for unauthorized reading of information from a tag. As RFIDs often have light cryptography schemes (if any), powerful back-end systems could potentially break the encryption in minutes, making the security protection ineffective.

9) Worms, viruses and malicious code: Worms, viruses and malicious code are a part of our daily cyber life. They are a prevalent and effective way of disrupting systems. Even very simple RFID tags, such as those used for tagging goods, can carry a malicious code [6].

10) Unauthorised access to / deletion / modification of devices / data: This attacks refers to unauthorized access to data stored on RFID, smart cards (especially contactless) and personal devices. Also databases can be subject to attacks through the network, as well as data can be illegally accessed and modified by unauthorized personnel.

11) Procedures / instructions not followed: This threat arises when, for example, a passenger does not follow instructions and causes a jam in the automated passport/immigration control or smart corridor.
12) Function creep: Function creep occurs when data are used for other purposes than the ones for which they were originally collected for. For example, in the air traffic scenario, a car rental company doing some market analysis might approach an airport operator to gain access to its data on airport parking.
13) State surveillance on citizens: Unjustified political agendas often lead to excessive surveillance on citizens. Every described case (true or invented) dramatically decreases trust and acceptance of technology (especially biometrics, RFID).
14) Low social acceptance of devices / equipment / procedures: RFID is perceived by many people as a privacy threat. They have been called "spychips" [7]. Most of the concerns presented during an EU public consultation on RFID were related to privacy [8]. Also some biometrics have low social acceptance, especially fingerprints which are commonly regarded as linked to criminal investigations.
15) Profiling: The abundance of data collected and processed in the IoT can lead to the creation of user profiles (relating to consumer preferences, traveling habits, etc.) [9].
16) Exclusion of the data subject from the data processing process: The automatisation of the processes in the IoT threatens to exclude the data subject from the data processing process.

4. MAJOR RISKS AND CHALLENGES IN A NUTSHELL

We have seen how by following a comprehensive risk assessment approach the ENISA study has identified vulnerabilities for each of the assets, and threats that could exploit those, in order to determine the individual risks, as mentioned in the methodology paragraph above. Considering these results and also the scenario presented in the previous section, we would like to discuss here the major risks for such an environment. We think that these risks can be projected onto other prospective IoT application areas beyond that of transport and air travel considered here, such as smart energy and smart grid; i.e., this analysis can add to the already existing debate of such risks, offering also a solid methodological basis to identify these risks.

We have seen that IoT technologies involve an increasing number of smart interconnected devices and sensors (e.g., cameras, biometric and medical sensors) that are often non-intrusive, transparent and invisible. Moreover, as the communication among these devices, as well as with related services is expected to happen anytime, anywhere, it is frequently conducted in a wireless and ad-hoc manner. Next to that, the services become much more fluid, decentralized and complex. Consequently, the security barriers in IoT become much thinner and more difficult to distinguish. It also becomes much simpler to collect, store, and search personal information and link data obtained from various sources, thereby de-anonymising data in a way and thus endangering people's privacy. Moreover, there is a concern that personal information is increasingly handled in an uncontrolled manner. A major risk here is that data will be used for purposes others or in addition to those originally specified.

The individuals lose track and control of their personal data processing, and as data may be transferred in a seamless way from processor to processor, they may not know where, when, by whom and why their data are being processed. Transparency is thus a serious risk. Imagine Akira receiving personal advertisements in his cell, based on his transactions during his flight and before; "spamming" may exist in such an environment, and actually considering the potential of an IoT environment, it may as well receive greater connotations. Profiling and data mining is a key enabler for this; although it is an excellent tool to provide personalised services to individuals, it can become a considerable threat when used for purposes described above. And perhaps spamming people with advertisements of new products is bothering but still not that harmful; but profiling people based on their shopping habits, dietary preferences or health condition can lead to serious breach of people's privacy and have further social impacts. Since we are talking about an Internet of Things scenario, the collection of data and profiling are both facts and not necessarily negative per se. However, excessive data collection and profiling, will inevitably lead to social sorting practices for commercial or other purposes, leading to exclusion of people from accessing services. Like repurposing of data and mission creep, social sorting is an increasing temptation with increasing data collection. "Social sorting" is a term first used by Lyons to describe social classification of people based on various criteria, which was further enabled by surveillance technologies [9]. It may seem at first glance that social sorting enables governments to more efficiently provide services and to better target citizens who might be at risk, but closer examination shows that social sorting often comes with evil; consumers who are targeted because they offer better commercial prospects inevitably means that other consumers are ignored or

marginalised. Social sorting enables insurance companies, airlines and many enterprises to provide some deals to their valued customers and not to others.

The new technologies are also bound to be more complex, at least in the perception of older generations and people that are not that comfortable with the use of new technologies and applications, which indeed is an issue today. In our scenario, Akira is a young guy that is familiar with technology and likes to use it; what would be the case if Akira were a 65-year-old man who could not speak a word of English? There is thus a risk that lot of people might not feel engaged with new technology and even fill irritated with its complexity. This will cause frustration of the citizens and low acceptance by the society at large.

Albeit a well-known current risk as well, identify theft is a very important consideration. This risk involves, e.g., compromise, loss of function and theft of Akira's RFID-embedded passport and national ID card. Identity theft poses a risk not only to those whose identities are stolen but to commercial and governmental undertakings as well. For example, fraudulent use of Akira's identity may impact banks and credit card companies. Moreover, identity theft creates a social burden on law enforcement authorities who try to combat such fraud as well as policy-makers who are obliged to divert time and resources from more socially productive uses.

Especially because such a future environment will rely heavily on ICT infrastructures, there is a serious concern regarding security (confidentiality, integrity and availability) of these infrastructures. Unavailability of services may occur (in the scenario processes regarding failure of reservation, booking and check-in procedures), meaning failure to conduct the main business transaction processes due to, e.g., loss, theft, unauthorised access, use of rogue cards and/or readers, attacks, spoofing and incompatibilities of both RFID and non-RFID embedded credit, debit and/or payment e-cards and e-wallets. This will translate from serious inconvenience of the citizens, to high economic costs for companies and serious reputation issues and embarrassment for both companies and states, depending on the incident.

Last but not least, as we have seen already with all the technological developments, the rapid advance of technology is not in sync with the slower pace of the legislative processes, which may lead to serious legal gaps in a future environment of Internet of Things, particularly in the context of air travel. On the one hand, we would not want a legal framework that would be so strict as to impede the development of such a vision, on the other, such a prospective environment cannot be created and promoted in a "legal vacuum" [10].

5. RECOMMENDATIONS

It may seem from the analysis above and indeed by other analyses and discussions on the issues that the IoT vision presents an ominous future and as such perhaps it should be abandoned. We should however recall examples as the IoT scenario presented in the second section and how following our traveller Akira around in that prospective scenario seemed very desirable and positive. We need to keep both images in our minds. Especially since the potential of such a prospective environment is great, we need to proactively identify its challenges and adopt actions with a view to prevent them or to address them appropriately, so as to enable such a future and to enhance citizens' trust in these technologies. In short: we should be proactive rather than reactive. To this end, we present here some major generic recommendations for consideration by different stakeholders.

A. Security and privacy by design

The concept of security and privacy by design is nothing new and is being advocated for quite some time now; however, it is important to note that this is a very important step towards providing better services, while providing a certain level of assurance to the citizens regarding security and privacy. Further research should also be encouraged in order to examine the issues in relation to IoT deployments and to further extend security and privacy solutions. In particular, research is needed to support [2]: (i) proper trust management, (ii) end-to-end policy enforcement and efficient rights management in highly distributed systems, (iii) data disclosure, usage and purpose control, (iv) developing privacy-enhancing and transparency-enhancing technologies, human machine interfaces that allow individual citizens to communicate with their environment [10], (v) effective cryptographic techniques for devices/sensors with limited resources and privacy-preserving identity management and (vi) architecting privacy-preserving systems, applications and services, as well as retrofitting existing ones to enable privacy options. Towards the same direction, it is important that any decision on the introduction of new technologies and new procedures should be taken only after a privacy, security and technology impact assessment. Such frameworks should be developed by a joint panel with representatives comprising all stakeholders (industry, civil society organisations, legislators, technology experts, health experts, and data protection authorities). Having said that, the European Commission has already kicked-off a procedure to develop a Privacy Impact Assessment framework for RFID applications [11];

something similar should be further considered for the IoT case as well.

B. Make devices / technologies more user friendly, be 'inclusive'

A first step is to investigate the issues related to usability of security and privacy technologies, and consequently research and development in the related technical fields including human-device interfaces and assisted privacy policy (consent) specification and management. This should also address discriminatory or exclusionary aspects of how information is presented to citizens (including IT-illiterates). We would like to develop technologies that people use and not just for the sake of it, so their requirements should be a key consideration.

C. Technical recommendations [2]

a) Light cryptography standards: Recently, a lot of research has been undertaken on light cryptography in the context of RFID, and many new protocols have been proposed [12]. We recommend developing light cryptography standards and giving some time to the scientific community to test them before wide implementation. In addition, we recommend that the combination of light-weight cryptography protocols (for light-duty devices) and the regular cryptography framework (e.g., PKI - Public Key Infrastructure, for back-end infrastructures) should be analyzed and that implementation technology and testbeds (e.g., elliptic-curve cryptography mutual authentication RFID) be explored. A very important consideration in this is key management: such a holistic framework should identify the actors generating the encryption keys (private/public keys), how these will be distributed and who (which agencies/organizations/authorities) will eventually be given access to such keys when necessary (e.g., to find information/crosslink data about suspects) .

b) Multi-modal person authentication: Automatic authentication of people is key to efficient and secure operational procedures in the air transport system. Experiences show that current implementations of biometric systems still show some weaknesses, even if they in principle seem to be promising. Using multifactor authentication (e.g., password plus biometrics, biometrics plus token) has the potential to increase overall security. In the same way, multimodal biometrics (several biometrics used in parallel) will make the authentication process more robust to errors and circumvention. Another aspect is the option to increase system flexibility by providing alternative (spare) authentication factors, which can be used in those cases where the basic way of authentication is not available (e.g., iris scan could be used for persons not having fingerprints).

D. Re-evaluate existing business structures and introduce new business models

As we have seen in the scenario, future air transportation is bound to bring in devices/sensors/applications that generate data and create integrated business processes that were not possible before. This probably holds true for other IoT implementations and applications. This evolution is also bi-directional: while IoT encourages enterprises to perform vertical business process integration improvement, the process improvement itself also guides the evolution of the IoT implementation (e.g., where to put the sensors, what types of new readers are needed). More importantly, enterprises should regard IoT beyond mere incremental improvement and investigate totally new business models (e.g., new way of air transportation) to achieve strong competitive advantages.

E. Raise awareness / educate citizens

In view of the characteristics of this new environment, it is crucial to increase awareness and promote education of citizens on the security and privacy risks posed by these new technologies and ways to be prepared, as well as on the use of the new devices / technologies / applications. As even highly automated processes still require human operators, it is important to develop and provide adequate training and instructions, e.g., for airline, airport and other ground personnel (in our scenario). The training shall address how to use the new procedures and technologies (e.g., in our scenario smart devices, RFID-enabled frequent flyer cards, RFID-enabled luggage tags) for all relevant processes (e.g., check-in, boarding, luggage check). Also guidelines for handling contingencies (e.g., system failures, emergency or crisis situations) have to be developed.

F. Adopt an "end-to-end" approach for securing IoT/RFID applications

Appropriately mitigating IoT/RFID risks lies beyond securing the RFID tags; it actually extends from smart devices to readers, and back-end databases and supporting telecommunication infrastructure.

G. Reevaluate and redesign the legal framework

Finally, and in order to address the legal challenges mentioned above, it seems that the legal framework of privacy and non-discrimination will need to be revisited [10]. Key considerations in such a revision would be behavioural marketing and profiling, transparency requirements particularly regarding generating and applying profiles, and including effective rights of access and effective rights to contest the application of profiles.

6. CONCLUSIONS

We have considered a neutral prospective IoT scenario in air travel in order to visualise the future, and based on ENISA's comprehensive risk assessment work, we have projected the risks identified for this specific air travel scenario to IoT applications in general. In addition, we have provided a set of recommendations that can be seen as guidelines for future developments of IoT environments. The recommendations are generic and should be considered in view of enhancing the potential of future IoT scenarios; indeed, this work in itself and its inevitable limitations shows that such studies need to be performed for all applications areas of IoT. We have certainly presented many serious challenges and risks posed by such a vision: it is not however the purpose of the paper to scare people away from this prospective environment. Quite the contrary, especially since we see much potential in this vision, we find that it is imperative to keep on identifying the risks and also appropriate solutions in a proactive and comprehensive way, so as to enable the full benefits of these technologies in the future, especially when one considers the advantages it could bring in many domains such as energy, transport and health. We maintain that it is possible to mould such a future and improve and simplify such prospective scenarios; needless to say, it will take considerable effort, and various stakeholders from different sectors need to be involved but still we believe that it can be accomplished. One thing is for certain though: the technology per se is not to blame; it is in our hands to turn it into a blessing or a curse.

7. ACKNOWLEDGEMENTS

This paper is based on recent work performed by ENISA on the subject, and the technical report it produced as a result [2]. The invited presentation and paper produced was co-authored with Dennis K. Nilsson and James Clarke.

8. REFERENCES

[1] G. Santucci, "The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects.," http://ec.europa.eu/ information society/policy/rfid/documents/iotrevolution.pdf, visited February 2010.

[2] B. Daskala (editor), A. Bassi, J. Clarke, FC. deCoussin, S. Ioannidis, E. Kosta, P. McCarthy, H. Ming-Yuh, E. Neves, D. K. Nilsson, M. Petkovic, and P. Rotter, "Flying 2.0 -Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technolog" an ENISA report, 2010. Final report and Annexes I and II, available for download at the ENISA web-site: http: //www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/.

[3] "International Standard ISO / IEC 27005:2008 Information technology Security techniques Information Security Risk Management,", 2008.

[4] Z. Kfir, and A. Wool, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, 2005.

[5] H. Bar-El, "Introduction to Side Channel Attacks," Whitepaper, Discretix 2003 http://www.discretix.com/wp.shtml, visited December, 2009.

[6] M. Rieback, B. Crispo, and A. Tanenbaum, "Is Your Cat Infected with a Computer Virus?," in *Proceedings of the 4th Annual IEEE Conference on Pervasive Computing and Communications (PerCom)*, 2006.

[7] K. Albrecht, and L. McIntyre, "Spychips. How major corporations and government plan to track your every move with RFID," Nelson Current, 2005.

[8] I.Maghiros, P. Rotter, and M. van Lieshout (editors), "RFID Technologies: Emerging Issues, Challenges and Policy Options," EUR Technical Report, EC DG-JRC, IPTS, 2007.

[9] D. Lyon (2002). Surveillance as social sorting: Computer codes and mobile bodies. In D. Lyon (Ed.), Surveillance as social sorting: Privacy, risk, and digital discrimination, (pp.13-30). New York: Routledge.

[10] M. Hilderbrandt, and S. Gutwirth (editors), "Profiling the European citizen: Cross-disciplinary perspectives," Springer 2008.

[11] M. Hildebrandt, and B-J. Koops, "D7.9: A Vision of Ambient Law," a FIDIS report, 2007. http://www.fidis.net/fileadmin/fidis/deliverables/ fidis-wp7-d7.9 A Vision of Ambient Law.pdf.

[12] European Commission, "Commission Recommendation on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification," 3200 final, Brussels, 2009.

[13] Information Security Group, Universit Catholique de Louvain, "RFID Security & Privacy Lounge," http://www.avoine.net/rfid/, visited December, 2009.