periodica polytechnica

Transportation Engineering
38/1 (2010) 9–12
doi: 10.3311/pp.tr.2010-1.02
web: http://www.pp.bme.hu/tr

RESEARCH ARTICLE

Staff access control at airports

Katalin Emese Bite

Received 2009-10-01

Abstract

Since 2001 the aviation industry is continuously facing a growing problem of safety and security within air travel procedure. The restrictions had been taken seriously, new rules and technologies surfaced. Passengers are often defined as wrongdoers but the airport staff has much better conditions to do any kind of attack or pilferage. To avoid any possibility of attack the airport's staff have to be controlled and monitored. With the combination of video camera, Radio Frequency Identification (RFID) tag and biometrical identification it is solvable.

Keywords

Staff · access control · security · RFID · biometrics

Katalin Emese Bite

Department of Transport Economics, BME, Bertalan L. u. 2. Z ép. 411, H-1111 Budapest, Hungary

e-mail: bitekati@kgazd.bme.hu

Introduction

Today more and more business and leisure travelers are flying to their destinations, the airports are operating at their peak capacity to be able to satisfy the continuously increasing demand. Since the 11^{th} of September 2001 security is an increase concern at airports, the fight against the terrorist attacks is prevalent and more emphasis lies on ensuring the passengers' security during the flight procedure within the terminal building and on board. The security restrictions are taken more seriously and the security industry entered its golden age. There were rules before too, but they were not taken so strict. The world and the aviation sector fears of terrorist attacks, the industry is trying to implement the best technologies to detect explosives, suspicious articles and behavior. Most airports, governmental and international organizations are aiming to introduce very strict security controls to reduce or eliminate any kind of threat to the passengers. In some way everyone is considered to be a potential terrorist or wrongdoer. The security staff's job is to recognize queer items, behavior. The security staff attends trainings related to recognize suspicious behavior and objects. The passengers have to bear much congestion, long queues at security check as this process is not too fast even if the industry tries to implement the quickest solutions. However, not only a passenger can be a wrongdoer or a terrorist, for staff member it is much easier to take anything inside airport's restricted areas. The airports' security service levels are evaluated by audits. In case the audit was unsuccessful, they give a time period and a list of the problems to the airport operators. The airport is fully equipped with video cameras but that is not identifying the people on screen. The security industry is constantly improving the level and effectiveness of the screening, trying to come out with new products which are more and more efficient in recognizing all kind of materials and things in a person's body or in a bag.

1 Today's security measures

In most of the world's airports everybody can enter the departure and arrival hall of the terminal building while the transit hall is reserved for passengers only after passing the strict rules of the border control and security check, the order depends on

the airport. Mainly in African (e.g. Kenya) or Asian (e.g. India) countries the visitors are not allowed to enter the terminal building, there are separate waiting halls next to the terminal. To enter the terminal building the passenger has to show the flight ticket and (together with his/her baggage) goes through a first security check. For example in Madras (India) the visitor can pay an extra fee to enter the check-in, but the waiting area is strictly separated from the check-in queue.

The terminal buildings are monitored by video camera and the people are informed of this monitoring by a sign at the entrance door: 'The building is monitored by a security camera'. Both passengers and baggage are passing through a security screening after the check-in to ensure that they lack any suspicious articles on board. After entering the Departure hall the movement of each person is recorded by a video until leaving the terminal. Some airports possess 360 degree camera, but this is new and still not common. The passenger, staff for restricted airport areas undergo metal detector test at security checks, in case of a problem the person will be checked separately, to speed up the manual check the staff can use the mobile metal detector. In some countries the passengers are checked twice.

The hand and checked in baggage, staff's belongings, cargo and postal matters pass through security checks of a 3D x-ray. The checked in baggage undergoes a security check right after check-in. Afterwards it can be directed instantly to the aircraft or it stays in a waiting position somewhere in the baggage sorting area. Transfer baggage passes through security control too after offloading from the aircraft at the baggage sorting before the new sorting would take place. But right before the luggage is taken to the aircraft; there is no extra security control. So it is easy here to struggle something into it or take out some items. That area is equipped with cameras but if the worker is with the back to the camera nobody sees what is happening.

The staff for restricted airport area has special authorizations for entering. Their past will be scrutinized for the last five year. The personnel working at the airport is passing through as strict security control as the passengers themselves by the same technology, they have strict entrance authorization and are watched all the time by a video camera. The authorizations are given according to his field of work, for the places he needs to have access to fulfil job well by the airport authority. The personnel of sensitive areas such as the baggage sorting or the cargo area have to be checked as well very strictly to avoid any mishandling (e.g. steal something from the baggage or the shipment, put something into it) of the baggage or shipment waiting for a flight.

The staff is having a smart card for identification. To enter a restricted zone he has to put his smart card next to reader placed in front the access of that area. If he has permission to enter the door opens, if not it stays closed. Anybody can use anyone's smart card as at the entrance there is just a card reader but without any other kind of personal identification (e.g. password, PIN code, biometrics). So in reality nobody really can be sure who enters the special area. The video camera inside the area is not showing who was entering just a person. And the person supervising the CCTV footage does not know everyone's access authorizations. To trick it out is very easy.

Some airports, especially in the USA are introducing biometrical identification parallel with the smart cards. The extra identification is placed next to the card reader before entering the restricted area. Most commonly used biometrical identification method for this is the IRIS recognition, facial recognition or fingerprint or their combination. The biometrical data are stored on the smart card and while supervising the access permission it is checked for matching and access permission.

Human factor can be the key to effective security but a weak link too. Not just the gullibility, good temper but money, good looking item, bribery etc. can lead to failure of the security restrictions and technologies. Lost uniforms and ID cards, repeated journalistic intrusions, incompetent screeners, and inoperative monitoring cameras are just sample examples how to trick out the security technology [6].

Many aircraft hijackings during the 1980's were easy to make it happen for the terrorist due to the complicity of the airport staff [6].

In December 2001 at Paris CDG Airport Richard Reid boarded a flight into the USA with explosive device concealed in his shoes. He could board the aircraft due to 2 reasons: the limitations of the metal detector and the laxity of the authority [6]).

In August 2004 two airplanes departing from Moscow's Domodedovo Airport were brought by 2 Chechen women. Not just because of the technology's failure, the police neglect and corruption allowed the activities of local mafia elements conducting regular criminal activity within the airport. The police officers were very cheap, they costed only US S170 [6].

Australian authorities identified airport staff as being behind drug trafficking at Sydney Airport in June 2005 [6].

In September 2005 at Vienna International Airport armed people went through the security check. Similar things happened in London, Warsaw, Philadelphia, Ottawa etc. [6].

2007 Royal Canadian Mounted Police inquiry claimed that 8 major airports were integrated into organized crime. Hundreds of police files and hundreds of people were involved in criminal activities, including 300 current or former employees [6].

Screening baggage is implemented to detect terrorist and their attacks but it also helped the growth of the airport-based criminalities to identify the items worth stealing [6].

2 Radio Frequency Identification as the new technology

Radio Frequency Identification (RFID) is a technology incorporated into a silicon chip that emits a radio signal which matches a user-defined serial number with an item. In this case the item is the personnel's badge. This number can be read at a distance by an antenna.

The main differences between the RFID and the smart card technology are listed below:

- The active tag is read by an antenna continuously, it does not need to be contacted physically to the reader.
- In case of passive tag it is the same, the only difference is that it will be only read in the field of the gate but it has not be contacted to the reader, so faster identification and access is feasible which is important in emergency situation.
- It is able to talk-write to a single tag allowing updating the status of the staff authorization anytime while the smart card needs to be changed.
- With an active tag the monitoring and tracing of the person is possible, the smart card only gives the information were he has entered.
- A map of his moving is possible to be generated by integrating it to a GIS, not just points of his entrances can be visualized.

The security of tags and databases raise important considerations concerning the confidentiality, integrity, and availability of the data on the tags, in the databases, and in how this information is being protected.

The aviation industry is already trialing RFID in the baggage handling, but it has unlimited features.

Another useful application of the RFID technology is for the access control of vehicle to airport operational areas [9]. At London Heathrow airport American Airlines' access control system prevents unauthorized drivers from using American Airline equipment as the driver can only start the vehicles engine by using Airport Security pass which is recognized by the use of RFID technology supplied by Vehicle Telematics Information System (VTIS) [7].

2.1 Using RFID tag for staff

The airport's terminal building and outside areas are full with video cameras recording the movement of the people passing by. On the video screen it is only possible to see that a person is moving but it is not possible to identify the person. In the USA some airports use facial recognizers implemented into the video cameras within the airport (especially where passengers are moving around). Today's technology is still not perfect in this regard. If the person who is passing by the camera is not looking directly into it or the total face cannot be seen even with zooming on it, then the facial recognizer is unable to identify the person. Even if it looks into the camera but something small has changed on its face (e.g. taking some pills to have the face deformed) or especially with bigger changes it is unable to identify the person. Even in the best case when the person looks into it, the facial recognizer needs to have a very high resolution to identify the person correctly, and the accuracy rate is quite low. The only reason for using facial recognition implemented into the video camera is that does not need physical contact and can be implemented in crowd situations [2]. In the future, ear shape recognition could be combined with facial recognition to identify the people from CCTV footage. Ear shape recognition has an accuracy rate of 99% according to laboratory test [2].

The staff's smart card only shows where he has entered but it is not giving a continuous information about his statement. It is getting more common within the aviation industry that the smart card is containing the biometrical information of the staff. These are varying between IRIS, facial or fingerprint recognition or their mixture.

Giving RFID tags embedded into badge combined with biometrical data of the laborer to the worker would secure the system. The video shows the movements of the staff viewed and his tag number shows who he is and if he is allowed to be there. At the entrance to a restricted area his authorization and personality is confirmed too or not depending if he is the badge's owner or not. Integrated into GIS software it can visualize differently and map of the movement flow can be drawn automatically. It is possible to store the data long time, in case of problems it is possible to find out who was there at that time. Time measurement can be taken too. For example if the staff is too long at a baggage, but he is with his back to the camera and there is later an announcement that something is missing from that bag, having the bags with RFID BagTags too, it is very easy to find out who made the crime.

In case of an emergency situation (e.g. pointing out a terrorist movement, putting something into a bag or aircraft) where the security personnel sees the crime in real-time on the monitor he can overwrite the wrongdoer's tag and cancel his authorization for exiting that area and the wrongdoer can be caught. The software can give alarms as well. In emergency situation it can map automatically where the alarm is and draw the quickest way to that place.

Of course the staff's privacy must be protected. The personal information of the staff member and his/her location should only be accessed by the security coordinator if there is a problem or the system is alerting an emergency situation. To avoid mishandling of the personal data a one-way code must be applied and the tag of the staff member should be only activated when it enters the restricted and authorization needed parts of the airport.

To ensure the staff's privacy rights apart the standardization further disposition can be made:

1 The tracking of the worker with RFID tag should facilitate the security issues of the airport and global industry. Due to privacy reasons the system on the monitor would only show RFID tag number. There is a need for 2 linked databases. First database contains the RFID tag number and access information, second one the RFID tag number and the passenger personal information. In case of trouble with a worker the second database opens automatically. The personnel at the monitoring must contact the security agent. The personal information of the worker should only be accessed by the security or po-

lice coordinator. Of course only authorized personnel would be able to access the database of the RFID tag and its current owner.

2 Attacks against the mishandling of the worker's RFID tag can be a radio signal which will be decoded behind the passenger by another person having a reader. To avoid this one-way code is a solution. A one-way code is a code, non-decodable for a decoder not having the special airport system code. Hence another person cannot retrieve any data from another passenger's tag.

3 The tag should be activated only when it enters a territory which requires authorization needed.

Airports should be the owners of the new technology and the authorization personnel could anytime change the permissions of each staff member. For the permanent staff a permanent card with RFID with the owner's biometrical information will be issued. For people rarely entering the airport's restricted area would get the card issued with every entrance, so the information on the card would be deleted automatically at the exit and for a new person re-used. The implantation costs and the tag prices are too high but the effort and money spent on aviation security is worth it. It is simpler to identify the violator and to take action immediately. It is much more efficient, less complicated to find out who is the violator.

2.2 Protection against baggage pilferage

In case of pilferage of the baggage a damage report must be filled. The claim department must consult frequently with the security staff to guard against fraudulent claims, summarize the experience, and distribute the summary with an emphasis on where the losses arose. Tracking luggage through the whole flight procedure with RFID tags enables to find out where the luggage was stored for how long time. Besides measuring the airport infrastructure it is a great method to measure if the airport personnel are pilfering the baggage or not. In case the luggage was stored at a place for long where nothing was around for a while, and afterwards the passenger reports that something is missing from the bag, the system can automatically track whole journey of the luggage to find out where it could have been tampered with. But this can be much better checked if the personnel is traced with RFID tag as well. The video camera of the baggage sorting, if it well placed, shows if one of staff is responsible for it, but it is not capable to show the person's identity. With the RFID the identity would be clear as well. One thing is to track passenger with RFID tags for flight security reasons to avoid that he is taking something suspicious on board; another is to make sure that none of the airport personnel is putting something secretly into the luggage of a passenger or into the baggage compartment.

3 Conclusion

Much time, effort and money is spent on improving the aviation security. Many times the people tend to think that the attacker or the offender can only be one or more passenger. In reality it is much easier for a staff member to smuggle in the drugs or any form of explosives into the restricted area of an airport and then continue it into an aircraft. Meanwhile the passengers are exposed stricter rules, long queues; hassle at the security check, the journey becomes less convenient. The airport to lower the queues and the proceeding time needs to implement and operate with more and more security infrastructure.

The costs generated by baggage loss, broken luggage or when something is missing from the hold baggage's content are very high for the airlines as they have to compensate the passenger for loss. The application of RFID technology would monitor the staff and take immediately the right action in emergency situations. With GIS software combined the emergency situations can be mapped on point and sent to the right people avoiding the problem. The airport can use the technology's infrastructure on different areas of the airport: baggage and passenger handling, cargo, ground support equipment etc., the features of RFID are unlimited which makes it in long term rentable.

References

1 *RFID for Airports and Airlines 2007-2017*, IDTechEx, March 2007.

2 **Griffiths S H**, *Biometrics: a role beyond staff identification*, Aviation Security International **15** (August, 2009), 29-32.

3 **Bite K E**, *Safety Baggage Reconciliation System planning at airports*, Budapest, 2005. MSc. Thesis.

4 **Beliczay T**, *A radiofrekvenciás azonosítás (RFID) központi eleme: a bélyeg*, Transpack (December 2005), 24-26.

5 *Aviation and Transportation Security Act*, 2001.

6 **Establier A**, *Airport Staff Access*, Aviation Security International **15** (February, 2009), 37-40.

7 **Ornellas T.**, *On the right track*, Ground Handling International **12** (October 2007), 38-42.

8 **Wilkinson Ch.**, Airports International (January 2009), 28-31.

9 **Pilling M.**, *Security Spin-off*, Airport World **6** (December 2001), no. 6, 44-46.

10 **Kővári B**, *Modern crew management methods in air transport*, Periodica Polytechnica, Transportation Engineering **31** (2003), no. 1-2, 3-16.