Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

Advanced Registered Traveler Paradigm using Dynamic Risk Profile and Multimodal Biometrics

Pravir Chawdhry and Rui Pareira Da Silva
Institute for the Protection and Security of the Citizen
Joint Research Centre, European Commission
21027 Ispra (VA) Italy
{Pravir.Chawdhry, Rui.Silva}@jrc.ec.europa.eu

***Abstract*—Registered Traveler (RT) program is an automated border control tool to reinforce homeland security without compromising convenience. This paper introduces a process-based approach for dynamic risk assessment using fuzzy logic in the RT program. We propose the use of multimodal biometrics for strong identification and greater interoperability with legacy schemes. The concept is applied to the passenger departure process in an airport. The conceptual framework has been prototyped in a laboratory-based demonstrator and deploys face and fingerprint modalities along with match-on-card biometric identification.**

***Keywords*—registered traveler, biometrics, identity, security, risk, trust, fuzzy logic, airport travel process**

I. INTRODUCTION

Security of air travel is a major concern for the citizens and governments. New technological measures have been introduced in recent years for rigorous identity checks and baggage screening of passengers at airports. However new security measures cause operational side effects in additional costs and processing time as well as passenger inconvenience.

To overcome bottleneck in passenger processing, Registered Traveler (RT) or Trusted Traveler schemes are being devised to increase throughput for low risk passengers. These schemes deploy biometric identification such as fingerprint recognition, for automated processing in self-service lanes. However most schemes tend to be stand-alone and may vary in terms of their scope and flexibility to respond to changing security threats in real-time. An end-to-end travel process is rarely taken into account, an exception being the miSense scheme [1].

Moreover, RT schemes tend to focus on purely the identity-based risk rather than assessing risk based on a combination of identity and intent, though the latter has become an active area of research [2]. RT schemes are also based on static trust: once accepted, RT scheme members can enjoy the low-risk status for 2-3 years.

Trust credentials and identity management in RT schemes use biometric tokens, though normally only a single biometric such as fingerprint or iris is deployed. The schemes being standalone and using diverse biometrics, tend to lack interoperability. Therefore whereas on its own an RT scheme may offer convenience, frequent business traveler may find them cumbersome, as they would need to carry several RT cards in their wallet. Since no single biometric is considered be ideal (in terms of universality, convenience, acceptability, stability, security and performance) multimodal biometric solution is thought to offer a more robust approach [3].

This paper presents an advanced Registered Traveler scheme using two concepts: (i) robust identity management based on multimodal biometric and biographic data; (ii) risk assessment for an individual based on a dynamic trust model. The scheme is based on the airport departure process for which we have adopted the Simplifying Passenger Travel (SPT) model [4]. The scheme has been implemented as a laboratory prototype.

The paper is organized as follows. In Section II we review the connected airport journey concept with the underlying SPT ideal process flow model and current RT schemes. In Section III we present a modified RT scheme along with our dynamic trust model for the travel process. Section IV presents our laboratory-based prototype. Finally, we present conclusions of this research in Section V.

II. THE CONNECTED AIRPORT JOURNEY

The connected journey concept exploits the identity management for convenience and security in the travel process [5]:

"*To collect and verify traveler's identity information as early as possible and by using the same information throughout the remainder of the airport journey to facilitate easier air travel while maintaining high standards of security and identity management.*"

The underlying tools to realize the connected journey are SPT ideal process flow model and the RT scheme, explained below.

A. SPT Ideal Process Flow

SPT is an IATA initiated program in partnership with airports, airlines, government authorities, ground handlers and technology suppliers [4]. The aim is to simplify passenger travel by streamlining and automation of passenger processes for air travel while addressing related security concerns.

SPT has defined the Ideal Process Flow (IPF) as a basis for its stakeholders to achieve the above aim. The IPF outlines an ideal view of passenger processing in air travel on the medium term (5-10 year horizon). It presents a detailed view of

978-1-4244-2794-9/09/$25.00 ©2009 IEEE

departure, arrival and transfer processes including the interactions between activities of the airline, the passenger, government authorities and baggage handler. The IPF aims to leverage on current technologies and international standards to achieve the objective of a connected journey. Fig. 1 gives a high-level abstraction of the IPF departure process from the passenger's perspective. The detailed process model can be seen in the IPF specification [4].

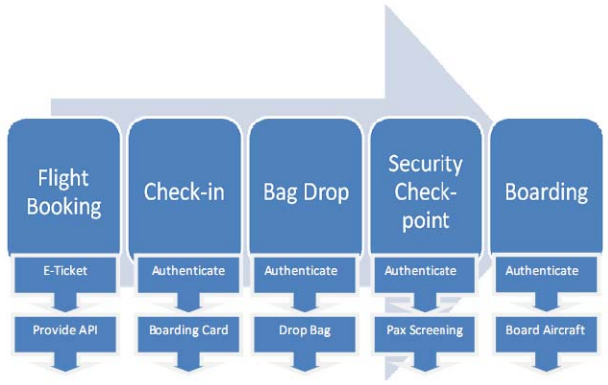


Figure 1. High-level abstraction of the Ideal Process Flow Departures Process (Passenger's view)

B. *Security of the SPT/IPF Process*

Security in the Ideal Process Flow is treated implicitly rather than explicitly. Whereas an information system perspective of security has three formal security requirements: confidentiality, integrity and availability [6], the process perspective of security is somewhat broader and formally less developed.

To deal with airport process security, we take a workflow based approach to process management. We propose that a passenger may be viewed as a *workflow item* of the departure or arrival process. For the security of these processes, therefore each workflow *item* must be handled in a formally secure manner[1]. The instantiation of a workflow item occurs with the flight booking activity i.e. when a person becomes a booked passenger.

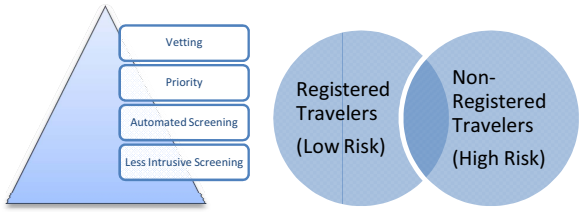
Once defined in such a way, the passenger process security requirements can be defined in terms of the classical *confidentiality-integrity-availability* model. In particular, integrity of the passenger process requires, among other things, that integrity of each workflow item (i.e. the passenger) is ensured. This requirement translates into the need to establish the identity of the passenger at the time of instantiating a new workflow item and then authenticating it throughout the entire travel process.

The use of biometric identification in registered traveler schemes, defined in the next section is a means for fulfilling the integrity requirement by strong authentication of a person's identity.

[1] Another process security requirement is that workflow definition and its implementation be subjected to integrity criteria.

C. *RT Scheme*

The motivation behind Registered Traveler or Trusted Traveler schemes is a combination of needs for increased border security alongside fluent travel facilitation for bona fide passengers. The underlying principle of RT scheme is to separate potential travelers into low-risk and high-risk passengers, as shown in Fig. 2. The low risk status is accorded based on the security vetting and previous travel history of a person. Once admitted to the scheme, the low-risk status remains valid for a fixed period (say, 2-3 years) during which the scheme member can benefit from facilitated security checks and border control in automated self-service lanes.



(a) (b)

Figure 2. (a) Registered Traveller Paradigm; (b) Binary-value risk classification in RT

One of the necessary conditions for a RT scheme to work as intended is that only the entitled members are able to take the benefit of the scheme. Therefore it should be virtually impossible for a non-member to use a genuine RT credential issued to someone else. This problem has been resolved by the use of biometric identification of all scheme members. Table I shows a few examples of RT schemes in operation or run as pilots in recent years, along with the types of biometrics used. An overview of European RT schemes is given in [7].

TABLE I. EXAMPLES OF REGISTERED TRAVELER SCHEMES

Scheme Name	Scheme Details		
	Geographical Scope	*Functional Scope*	*Type of Biometric*
Nexus	USA/Canada	border	Fingerprint
RAPID* #	PT/RoW	border	face
Privium	NL/RoW	border	iris
ABG	DE/RoW	border	iris
Pegase	FR/RoW	border	fingerprint
IRIS	UK/RoW	border	iris
miSense	UK/RoW	border	finger
miSense-Plus	UK/Hong Kong	border	face, iris, fingerprint
SmartGate * #	Australia/NZ	border	face

* No separate enrolment is required

The scheme uses biometric passport as reference token

RoW = Rest of the world

There are two main criticisms of this approach. Firstly, the assigning of low-trust profile for a fixed-period can be misused by the 'sleepers' who would otherwise have a clean sheet to be able to pass the vetting process. Secondly, the identity

verification based on a single biometric is not sufficiently risk-free, though the iris biometric is considered relatively more secure in terms of false match or spoofing [8].

To avoid a false sense of security, therefore RT schemes need to be improved. We propose here the use of dynamic risk assessment in real-time, along with the use of multimodal biometrics to address the two concerns mentioned above.

III. An Advanced Registered Traveler Scheme

A. *Multi-valued Trust*

Instead of a static value of trust (inversely, risk), we use a dynamic trust model in real time, based on known passenger data and current intentions.

The issue of determining risk related to passenger's intent is an active research area [2]. We use an evidential reasoning model based on three threat variables: current information on the passenger, handbag search and body scan results.[2]

$$trustlevel(p,k)=f(paxinfo(p,k),\ handbag(p,k),\ bodyscan(p,k)) \quad (1)$$

where p is the passenger index and k is the discrete time index.

The feasibility of the evidential reasoning model is based on the following argument. Current intelligence information is already used in taking *'clear to board'* decision through APIS and passenger manifest obtained before the departure and is therefore state-of-the art. Likewise, handbag search and body scans are used before permitting entry to the secure area. However, results of these scans are currently not linked to specific passengers even though the potential of linking them does exist through the bar-coded boarding card which is inspected at the security checkpoint. The SPT model in Fig. 1 envisages the use of identity control at the security checkpoint. It is also possible to pinpoint the types of prohibited items in handbag or on person from the scanned images. Therefore we consider it a logical next step to automate the generation of individual threat profiles of handbag search and body scan. What remains then is the synthesis of a joint risk (trust) profile by linking the three currently isolated bits of information on the threat variables in (1) using a decision theoretic approach.

The reasoning model is implemented in MATLAB using fuzzy logic. Fig. 3 shows the formulation of trust profile based on the three primary threat variables: passenger information, handbag scan and body scan. Fig. 4 shows how different levels of threat from the three primary variables are combined in real time to determine the overall dynamic risk (trust) level. We call this risk profile dynamic in the sense that it is based on specific (discrete) samples of body scan, handbag search and intelligence database query. Fig. 5 shows the surface profile of trust level as a function of input variables, after defuzzification. The techniques for fuzzy modelling are explained in [9].

We chose fuzzy logic to model risk because it represents the heuristics applied by human experts and likewise is amenable to learning new rules and adapting to novel situations. The risk model, i.e. the choice of input variables and fuzzy rules for calculating the trust level can be modified based on the experience, expertise and policy of the security process owner. Moreover, fuzzy logic based decision models are easy to implement in embedded environments for real-time application.

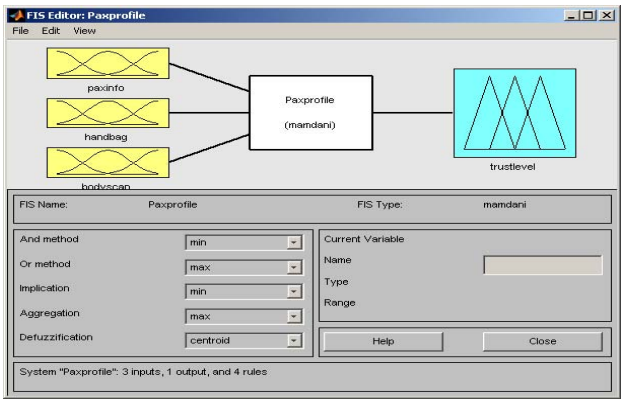
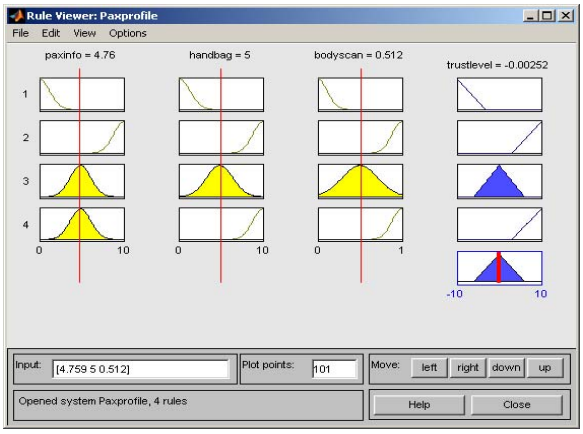
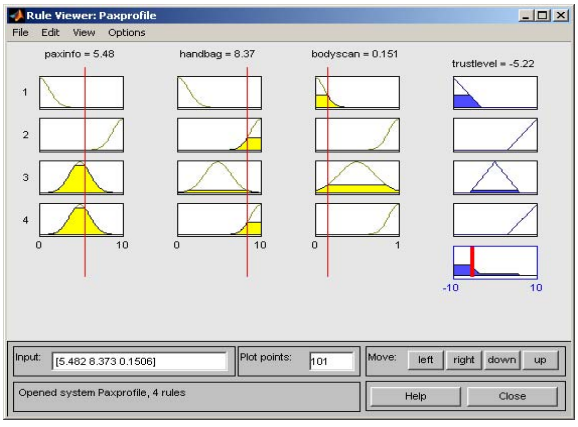


Figure 3. Dynamic risk profile (trust level) based on fuzzy logic



(a) Average trust level



(b) Low trust level

Figure 4. Passenger risk profile (*trust level*) determined from passenger information, handbag search and body scan

[2]Eventually, baggage scan results could also be included in the model.

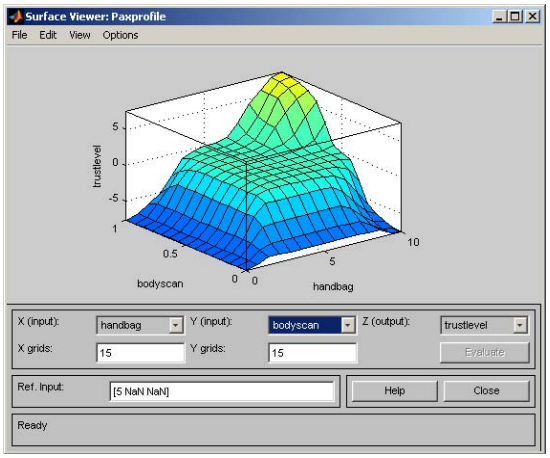


Figure 5 (a). Surface plot of dynamic trust as a function of body scan and handbag search

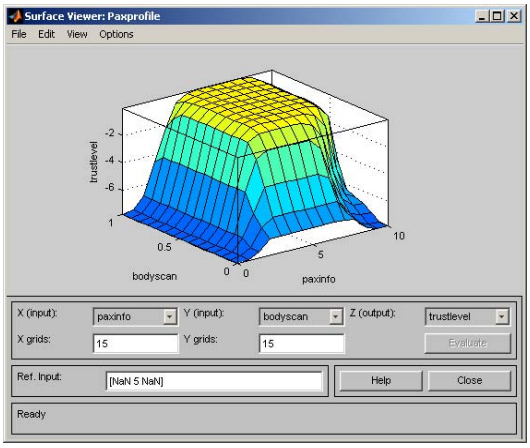


Figure 5 (b). Surface plot of dynamic trust as a function of body scan and passenger information

B. *RT Scheme with multimodal biometrics*

In order to strengthen biometric authentication, the improved RT scheme is based on multimodal biometrics. We have so far implemented face and fingerprint biometrics and additional biometrics modalities, e.g. iris, can be conveniently added in the modular design. The use of multiple biometric modalities has an additional advantage of offering backward compatibility and potential interoperability with single-biometric based schemes currently in operation.[3]

Moreover, in contrast to the traditional RT schemes which are mostly point-based, i.e. dedicated to specific control points such as border control or access to secure area, our scheme is process-based, spanning the entire departure process. Therefore each stage of the departure process workflow is aware of the progress of a passenger in the preceding stages and their current risk level. This ensures the workflow security in that a passenger can proceed to the next stage if and only if all the previous actions have been successfully completed and stipulated security pre-conditions are satisfied. For example, an action cannot be repeated by an imposter e.g. gaining access to the security area using a duplicate/invalid boarding card.

The scheme, shown in Fig. 6, consists of several features:

- Enrolment with biometric and biographical data
- Multiple biometric modalities (face and fingerprint)
- Dedicated RT flight booking site for scheme members
- Self-service check-in (online or kiosk)
- Bar-coded boarding pass for access to security area
- Option to use biometric match-on-system or match-on-card (for increased privacy protection)
- Flight database for booking, check-in and secure area access control
- Booked passenger database
- Government security database for vetting.

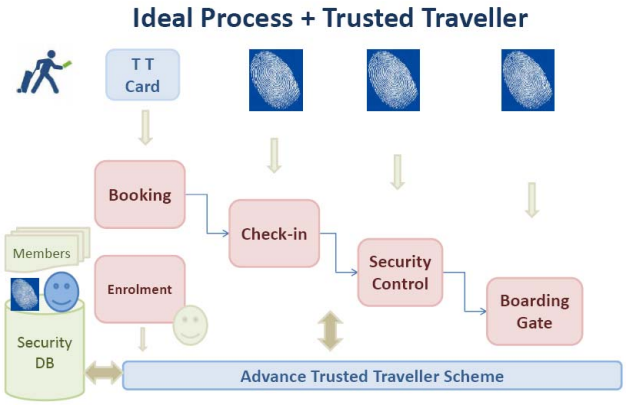


Figure 6. An advanced RT scheme based on SPT Ideal Process Flow model and multimodal biometrics

IV. System Prototype

A. *Requirements Engineering*

For our RT demonstrator all passenger-related activities of the Ideal Process Flow of the SPT model have been implemented, excluding the bag drop, but including the actions by authorities in fulfilling the registered traveler enrolment role. Main elements of the demonstrator are shown in Fig. 7. Software systems requirements were defined using a formal process, as shown by examples in Fig. 8-10.

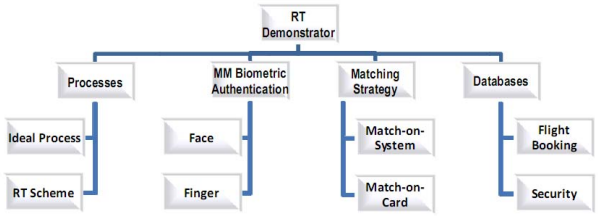


Figure 7: Main elements of the prototype Registered Traveler Demonstrator

[3] In practice, interoperability is a system integration issue as well as that of standardization at the level of biometric sensors, image encoding, feature templates, biometric matching algorithms and middleware APIs.

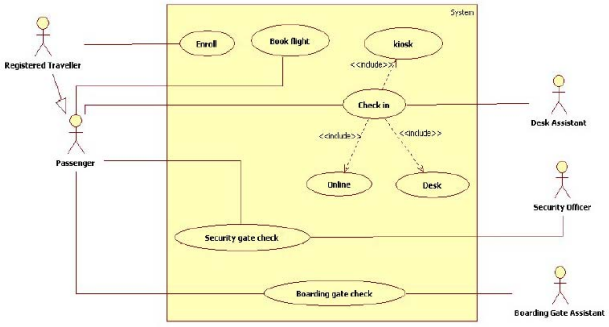


Figure 8. Use case for the Registered Traveller prototype

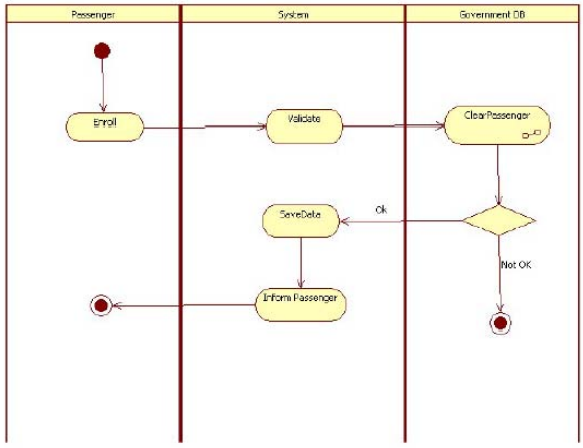


Figure 9. Activity Diagram of the Enrolment process

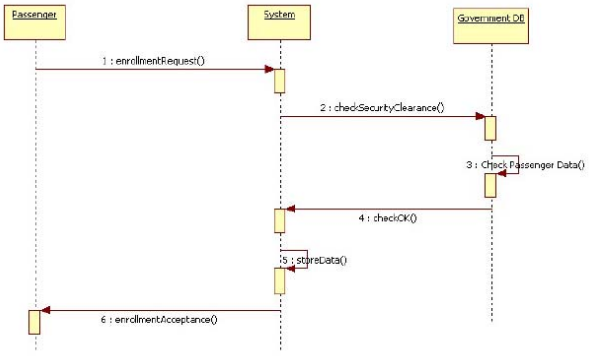


Figure 10. Sequence Diagram for the enrolment process

B. *Software Prototyping*

In the present application prototype, a common database has been implemented for passenger data and flight information, and there is also one representing governmental database of a black list of persons.

Different user interfaces are defined for each stage of the passenger departure process as described in the SPT/Ideal Process Flow.

Passenger Enrolment:

The passenger enrolls with his personal biographic data as well as his biometric data and becomes a member of the registered traveler program. As a result, he receives his login credentials so that he can manage his trusted flight bookings subsequently. Optionally, he also receives a personal RT card which is a smartcard with biometric match-on-card facility.

Flight booking and management:

This part of the prototype consists of a small web portal which uses web components of .NET framework, to allow online booking. In the web portal the RBAC security model of .NET framework has been incorporated to allow distinct roles such as system administrator and the end-user. User management is done using ASP.Net security tools.

The portal allows authorized administrators to manage the basic flight database. Registered travelers can login into the portal and utilize flight booking facility and subsequently review details of their booked flights.

Flight Check-in, Security Checkpoint, Boarding Gate:

The RT member can check in online or at the airport, either at the check-in desk or at a self-service kiosk. Having done so, the passenger gets the boarding card and can proceed to the security check point. Access to the restricted area through the security control requires biometric identity verification as well as scanning of the bar-coded boarding pass for its current validity and single use status. The final step is to proceed to the boarding gate before getting on the plane.

In all the above mentioned steps (check in, security check and boarding gate) the passenger's identity is verified biometrically (facial image and fingerprint matching) along with the relevant flight reservation details and biographic data. In addition, passenger's personal and biometric data is cross-checked with the government database to flag black listed persons. Figs. 11 and 12 show the screenshots corresponding to initial RT enrolment and subsequent identity verification at security control based on fingerprint and face biometrics.

C. *Implementation Infrastructure*

Prototyping has been done using Microsoft .NET development platform, and Megamatcher SDK components from Neurotechnology for biometric enrolment and verification [10]. Megamatcher has a client-server based multi-modal biometric software architecture, suited for our application, with finger and face biometrics algorithms. The platform also offers cluster based scaling up option.

The biometric sensor devices include 2MPixel webcam, Digital Persona URU4000 fingerprint scanner, and RTScan barcode reader compliant with IATA's bar coded boarding pass specification [11].

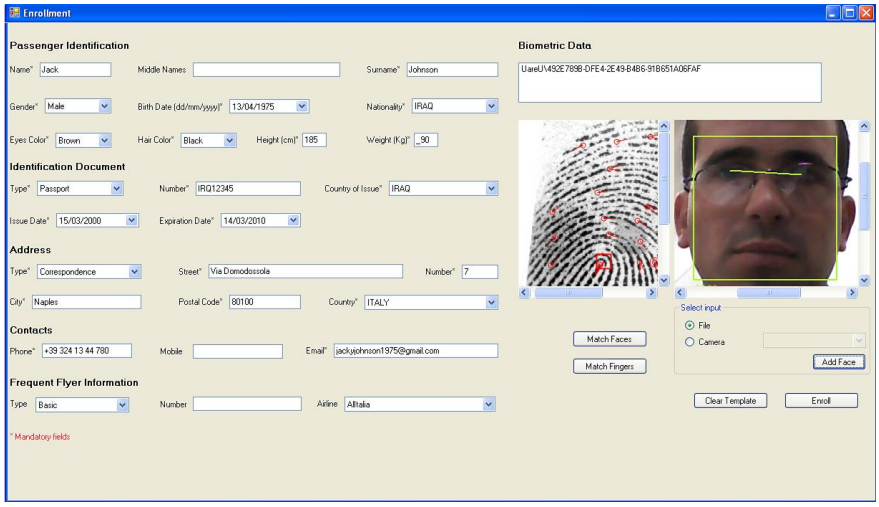


Figure 11. Registered Traveller Enrolment screen in the RT prototype. The left part of the screen shows the biographical data of the holder whereas the right part of the screen shows the facial image and fingerprint biometrics.

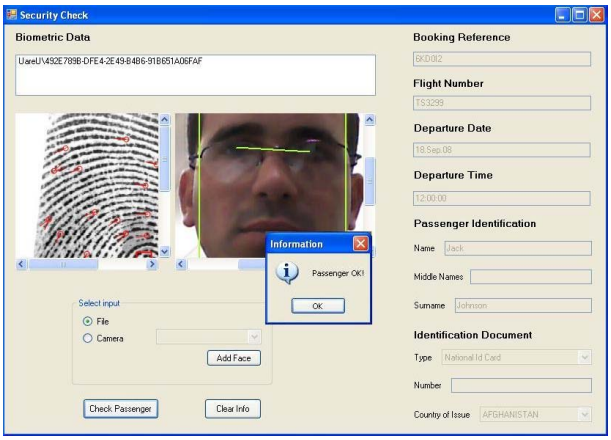


Figure 12. RT Prototype: Biometric verification at security checkpoint

V. CONCLUSIONS

New security threats in airports have given rise to a need for risk-based passenger screening. Current risk assessment process is fragmented and does not take advantage of integrating diverse risk-related information on passengers in real time. This paper has presented a framework for combining three primary threat variables in real time and deploying the resulting risk metric in a seamless process context, the advanced Registered Traveler scheme. The proposed scheme is based on the biographic data, multimodal biometrics and dynamic risk (trust) profile. A simple intent model based on fuzzy logic was included in the risk profile.

Main contributions of this paper are: (i) the use of a dynamic risk model of passengers based on fuzzy logic that integrates fragmented risk data; (ii) the use of multi-biometrics and biographical data for secure identity verification in a seamless process of Registered Traveler.

In future work, the dynamic risk profile algorithm can be modified by varying weights and even including multiple samples over a period of time, based on the specific security policy of airport security authorities. Similarly, the intent model may be made more sophisticated based on the available real time sensor/scanner data. This approach would help the RT scheme to develop self-learning capability.

ACKNOWLEDGMENT

This work was carried out under the JRC/IPSC Exploratory Research grant.

REFERENCES

[1] BAA, *miSense – the Connected Journey*, http://www.misense.org

[2] DHS, Deception Detection: Identifying hostile intent, http://www.homelandsecurity.org/snapshots/newsletter/2007-05.htm

[3] A. Ross, K. Nandakumar, A.K. Jain. Handbook of Multimodal Biometrics, Springer, 2006, ISBN 978-0-387-22296-7.

[4] SPT: Ideal Process Flow V 2.0, 1 December 2006, http://www.iata.org/NR/rdonlyres/31BD66A2-4446-4514-A911-3EA9DDAC7CAA/0/IPF_V20_FINAL.pdf

[5] A. Gupta and I. N. Sneddon, "Simplifying passenger travel (SPT) program," Third symposium oand Exhibition on ICAO MRTDs, Biometrics and Security Standards, Montreal, October 2007.

[6] BS7799-3:2005, Information Security Management Systems - Guidelines for Information Security Risk Management, http://17799.standardsdirect.org/bs7799.htm

[7] BIOPASS, "Study on Automated Biometric Crossing Systems for Registered Passenger at Four European Airports", Frontex Technical report 2008, ISBN 978-92-95033-00-9.

[8] J. Daugman, "How Iris Recognition Works", http://www.cl.cam.ac.uk/~jgd1000/csvt.pdf

[9] L H Tsoukalas and R E Uhrig, Fuzzy and Neural Approaches in Engineering, John Wiley, 1997, ISBN 0-471-16003-2.

[10] Megamatcher SDK, http://www.neurotechnology.com/mm_sdk.html

[11] IATA, Bar coded boarding passes (BCBP) http://www.iata.org/stb/bcbp