Face Recognition-based Presentation Attack Detection in a Two-step Segregated Automated Border Control e-Gate
Results of a Pilot Experience at Adolfo Suárez Madrid-Barajas Airport

David Ortega del Campo, Cristina Conde, Ángel Serrano, Isaac Martín de Diego and Enrique Cabello

Computer Architecture And Technology, Computer Science And Artificial Intelligence, University Rey Juan Carlos, Tulipan s/n, Madrid, Spain

Keywords: Automated Border Control, Face Biometrics, Presentation Attack Detection, Security.

Abstract: This paper presents the pilot of a new Automatic Border Control system (ABC) that is being developed in the ABC4EU European project and that conform to the new laws established for the Schengen zone. These new ABCs have some specific characteristics, such as a structural configuration divided into two devices: self-enrolment kiosk and biometric gate, one for enrolment and the other one for verification, which entails two capture stages and two weaknesses where it is possible to attack the system. The tests were carried out with a pilot of the system, implemented at T4-S (T4 satellite) terminal of Adolfo Suárez Madrid-Barajas Airport. Our experiments have tested the security of the system by simulating several presentation attacks, at both stages of the system. For these attacks, different artefacts proposed in the literature about Presentation Attack Detection have been used. We present the obtained results with each of the attacks, indicating which may be more dangerous to the system and suggesting some countermeasure that could increase the reliability and security of the system.

1 INTRODUCTION

In a yearly report published by Boeing company, the foresight of the growth of aircraft passengers traffic worldwide reaches an amount of nearly 5% in the 2015-2035 period (Boeing, 2016). This increase is expected to double up to 9.5% for the specific area of South Asia in the same period. These numbers suggest that a huge effort needs to be done in the following years in security controls at airport border checkpoints. Other kinds of borders, such as those at seaports and land borders, are also expected to suffer from an important increase of traffic (Donida Labati et al., 2016).

Customs and border officers need to be provided with quick and effective procedures and tools to guarantee a comfortable queueless border crossing for passengers, while keeping control of the flow of people across the border.

Automated Border Control systems (ABC) are proving to be the better solution to these new challenges. It allows controlling the crossing of travellers in an automatic or semi-automatic way.

1.1 Automated Border Controls

With the launch of the Schengen Area in 1995, a policy of open borders was approved so the mutual borders of the participant states were eliminated and only the outer borders (this is, with non-Schengen countries) were kept. As of this writing, 26 European states belong to this area, of which 4 are not European Union (EU) members (this is, Norway, Iceland, Switzerland and Liechtenstein). Four more EU members are obliged to join in the future (Bulgaria, Croatia, Cyprus and Romania), while the United Kingdom and Ireland have opted to stay out. Three European microstates, such as Monaco, San Marino and the Vatican City, are *de facto* members. The whole Schengen Area comprises a surface higher than 4.3 million square metres and a population of almost 420 million people, who can travel from one member state to another without border controls.

On the other hand, passengers from non-member states, or third country national passengers (TCN), do have to cross a border control.

Since the Netherlands started a fingerprint recognition project for frequent passengers in 1992 at

Campo, D., Conde, C., Serrano, Á., Diego, I. and Cabello, E.
Face Recognition-based Presentation Attack Detection in a Two-step Segregated Automated Border Control e-Gate - Results of a Pilot Experience at Adolfo Suárez Madrid-Barajas Airport.
DOI: 10.5220/0006426901290138
In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT*, pages 129-138
ISBN: 978-989-758-259-2

Amsterdam Schiphol Airport, several other countries have included automated border controls (ABC). In particular, the European Union Frontex agency was founded in 2004 with the aim to improve the management of the outer borders of the state members. Frontex defines an ABC as an automatic system that performs three fundamental operations: (1) it authenticates the passenger's machine readable travel document (eMRTD, this is, electronic passport, national ID card, etc.), (2) it verifies the identity of the passenger as the legitimate holder of the document by means of a biometric procedure, and (3) it checks his/her permission to cross the border according the predefined rules. All of this is made with minimal or no human intervention at all (Frontex, 2012).

ABC systems make use of electronic gates (e-gates), which are architectural components that control the flow of passengers at the border automatically by means of moving or fixed elements, document reading devices and biometric feature capture devices. In particular, the passenger presents the eMRTD to the system scanner, which detects and extracts his/her personal data from the so-called machine-readable zone (MRZ) of the document (Figure 1). A query to the database of allowed-to-cross passengers is made and then, if succeeded, the biometric data of the passenger are extracted from the document's chip. These data can include a set of facial pictures, fingerprints, etc. The passenger then has to provide the ABC system with his/her biometric features at that very moment ("live samples"), which are compared with those read from the document. If it is a match, then the e-gate opens the doors and the passenger is allowed through the border.

Three possible configurations for an ABC e-gate can be used (Figure 2). First, one passenger at a time is made enter a mantrap, which is a cubicle with two doors. In this space, both the document authentication and the biometric verification are made in parallel in a one-step process, so this solution can be very fast. The other two configurations use a two-step process. On the one hand, integrated solution, on which the document authentication takes place just outside a mantrap, inside of which the biometric operation is carried out.

In a third configuration, segregated solution, the document authentication and the biometric verification is performed in an enrolment kiosk, while a second biometric verification is made at the one-door e-gate.

For more information on ABC, the reader should check Donadi Labati et al. (2016), which provide a survey on biometric recognition in ABC systems, while Sánchez del Río et al. (2016) specifically focus on face recognition-based ABC systems.

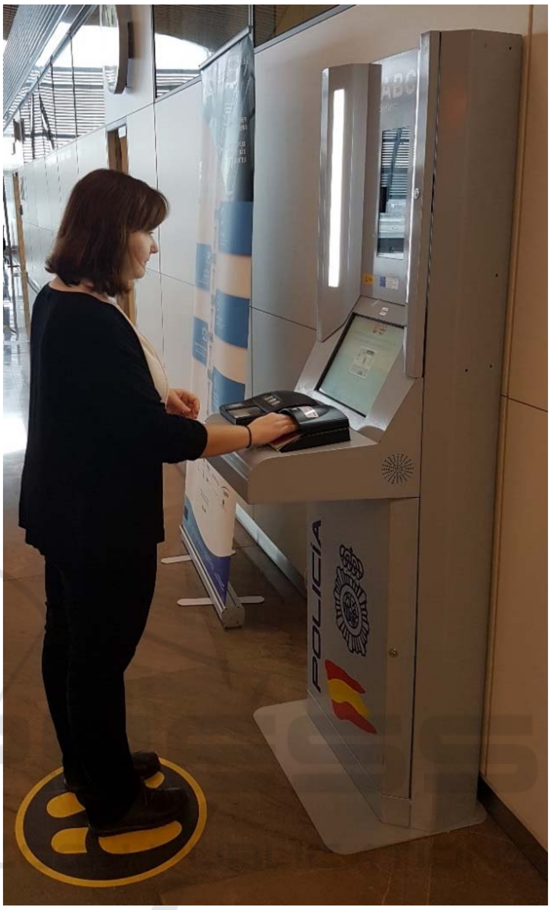

Figure 1: Example of an ABC. Picture taken from the pilot experience at Adolfo Suárez Madrid-Barajas Airport T4-S international arrivals terminal.

Several European projects are devoted to ABC e-gates. The results presented in this paper belong to the ABC4EU project (ABC4EU, 2014), from the Seventh Framework Programme. The details will be explained in Section 2. Other similar projects can be found in FastPass (2016), Berglund and Karbauskaite (2008) and Kosmerlj et al., (2006), to cite only a few.

1.2 Security Aspects in ABC Systems

Special attention has to be paid in order to guarantee that only allowed passengers cross the border through an ABC e-gate. There are two types of attacks on ABC biometric subsystems:

On the one hand, there are the attacks that take place in the eMRTD and consist of replacing or altering the biometric data stored on the MRZ of the passport. An example of this is the so-called morphing technique (Ferrara et al., 2014), where the biometric features (such as the face picture stored on the passport chip) of the passenger and of the attacker are combined to produce an intermediate image that would deceive the system. A possible improvement that could decrease these attacks is to step up security measures and encryption of documents.

Another type of attack is what is known as spoofing or presentation attack (PA). This type of attack takes place at the capture device and is based on the impersonation of the biometric features of the passenger by the attacker without having to manipulate any documents. When the passenger provides his/her biometric features collaboratively and interacts with the system in the expected way, this act is called a “bona fide presentation”. On the other hand, a PA occurs when a person tries to interfere with the normal operation of the system (ISO/IEC, 2016a).

Our study focuses on the second type of attacks, with genuine passports (no manipulation), where the attacker attempts to impersonate a passenger and uses his/her original documents.

The biometric feature or object used in the attack is called presentation attack instrument (PAI). Examples of PAIs include a photograph of a face (printed in paper or displayed on a screen), a 3D face mask, a fake finger made of plastic, or even a real finger from a dead body.

Presentation attacks can be classified into two classes (ISO/IEC, 2016b). In the first one, presentation attacks make use of human-based PAIs, including parts of a dead body, features intentionally modified (scars, surgery, temporal changes induced by medication), impersonation of someone else’s feature, accidental match of someone else’s feature in a bona fide presentation (zero effort impostor attempt), or genuine feature presentation obtained under coercion or menace.

A second kind of presentation attacks employ artificial PAIs. These artefacts can be obtained directly from the real biometric feature, for example with a mold, or indirectly from a latent sample (a fingerprint left on a surface). The biometric feature can be also captured by a recording device, such as video-camera or a photographic camera. Sometimes a complete biometric feature can be synthetically rebuilt from a genuine template, or can be obtained with a specific software from another user’s feature.

Completely synthetic features generated without resemblance to a specific user’s features can be considered here too as an artificial presentation attack.

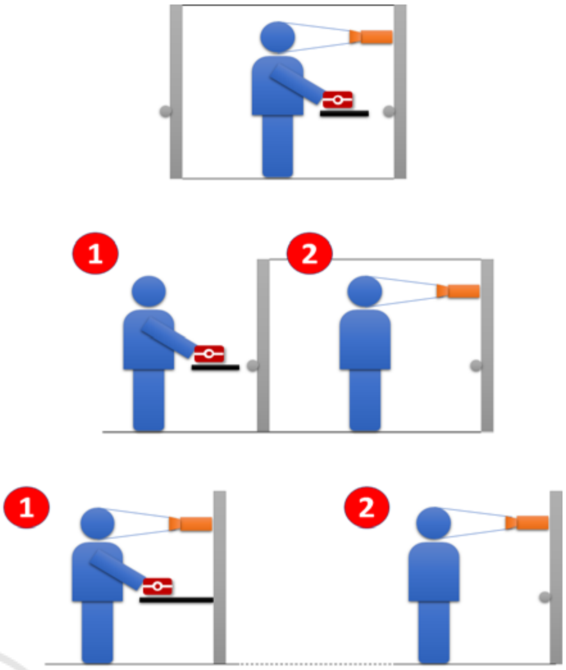

Figure 2: ABC topologies. From top to bottom: One-step ABC, two-step integrated ABC and two-step segregated ABC.

A “presentation attack detection” (PAD) is the automatic recognition of presentation attacks, which is performed by the so called PAD subsystem as a part of the ABC system. Within the PAD, some kind of liveness checking is needed, this is, the biometric feature is being acquired from a live user. Examples of liveness detection can include measuring the skin temperature, detection of blood vessels, eye blink, etc.

A biometric system can be attacked at different stages of the data flow: at the sensor, at the signal processing module, at the database, at the matching module, at the decision module, or in the intermediate points (Ratha et al., 2001; ISO/IEC, 2016a). For the PAD subsystem, only attacks at the sensor level are analyzed, this is, at the e-gate.

1.3 Evaluation of the Performance of a PAD Subsystem

When a person tries to cross an e-gate, his/her biometric features are provided to the PAD subsystem. These features are analyzed by the system’s algorithm, which has been trained in advance in order to be able to tell apart real passengers from attackers (identity impersonators). The result of the PAD subsystem is a score of confidence on whetther fact that the presentation of the biometric features was genuine or fraudulent. The final decision (response) is made by comparing this score with a classification threshold obtained during the training process or set as a function of security needs.

So far, PAD have been evaluated with usual biometric systems measures, like FMR (false match rate) or FNMR (false non match rate), but latest standards propose an evaluation of the performance of the PAD subsystem computing two kinds of metrics (ISO/IEC, 2016b). The first one is the ratio of bona fide presentations incorrectly classified as attacks (called "bona fide presentation classification error rate", *BPCER*). Suppose we consider N_{BF} as the total number of bona fine presentations. Let Res_i be the response of the PAD subsystem to the *i* presentation ($1 \leq i \leq N_{BF}$). This value is equal to 1 if this bona fide presentation is classified as an attack, or 0 otherwise (it is correctly identified as a bona fide presentation). Then *BPCER* can be calculated as follows:

$$BPCER = \frac{\sum_{i=1}^{N_{BF}} Res_i}{N_{BF}} \qquad (1)$$

The second metrics for the evaluation of the PAD subsystem is the ratio of attacks incorrectly classified as bona fide presentations (called "attack presentation classification error rate", *APCER*). In this case, let N_{PAIS} be the number of attack presentations for a specific PAI species (PAIS), this is, for a set of PAIs produced with the same method and based on different biometric characteristics. In this case, *APCER* can be computed with the following equation:

$$APCER_{PAIS} = \frac{\sum_{i=1}^{N_{PAIS}}(1 - Res_i)}{N_{PAIS}}, \qquad (2)$$

where Res_i is the response of the PAD subsystem to the *i* presentation ($1 \leq i \leq N_{PAIS}$). This value is 1 if this attack presentation is classified as an attack, or 0 otherwise (it is wrongly identified as a bona fide presentation). Bear in mind that this *APCER* value has to be computed for every PAI species.

The accuracy of a system can be measured using an Average Classification Error Rate (*ACER*) defined as:

$$ACER = \frac{(APCER + BPCER)}{2} \qquad (3)$$

As with regular biometric systems, both kinds of errors, *BPCER* and *APCER*, cannot be minimized at the same time, as when one decreases, the other one increases, and vice versa. This is due to the fact that the response of bona fide presentations cannot be completely separated from the response of attack presentations.

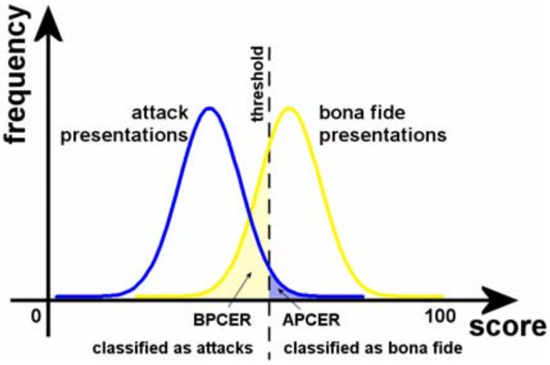

Figure 3: Histograms of classification for bona fide presentations and attack presentations. The shaded regions correspond to classification errors. The height of both histograms has been drawn equal for the sake of clarity.

If we suppose that bona fide presentations tend to receive higher classification scores from the PAD subsystem and attack presentations tend to obtain lower values, there is usually an overlap between both score histograms that cannot be solved (Figure 3). Due to the selection of a specific threshold, classification errors occur.

As can be seen, all the bona fide presentations with a score lower than the chosen threshold will be incorrectly classified as attacks, and therefore they will contribute to the *BPCER* computation. On the other hand, all the attack presentations with a score higher than the threshold will be incorrectly classified as being bona fide presentation. In this case, they have to be included in the *APCER* computation.

A good way to determine a good acceptance threshold would be to choose the threshold in which the *BPCER* and *APCER* values are the same. We shall call this value the "Equal presentation classificacion error rate" (*EPCER*).

The rest of this paper is organized as follows. In Section 2, we describe the ABC4EU project and its security peculiarities compared to the rest of the ABC systems. In Section 3, our experimental setup in a pilot experience performed at Adolfo Suárez Madrid-Barajas Airport in December 2016 is explained, while Section 4 provides our results and their analysis. Finally in Section 5 our main conclusions are summarized.

2 ABC4EU PROJECT

Within the Seventh Framework Programme of the

European Union, ABC4EU project is a four-year collaborative effort to enhance the workflow and functionalities of ABC e-gates for all kinds of borders (airports, harbours and land borders), to identify the problems of the current ABC in Europe and to define the requirements of these systems for Schengen passengers (ABC4EU, 2014). Several institutions of eight European countries (Estonia, Finland, Germany, Ireland, Italy, Portugal, Romania, and Spain) belong to the project.

The ABC4EU project must primarily conform to the rules defined in the Schengen Border Code (SBC), which establishes standards, protocols and procedures for travellers in the Schengen Area. Although one of its main objectives is security, it also takes into account the regulation on data protection established by the EU and by each country in particular, defined in the Recommendation and Data Protection Directive 95/46/EC. The system handles two important databases with very sensitive information: VIS (Visa Information System), which contains biometric information, and SIS (Schengen Information System), with information on criminal activities.

With the Schengen agreement, the controls were transferred to the borders with third countries, so the ABC4EU project focuses on TCN travellers. These travellers may be in two legal situations: travellers without the need of a visa (TCNVE, Third Country National Visa Exempt), or those with a visa or a residence permit (TCNVH, Third Country National Visa Holder). For each of these types of travellers there is a different procedure defined in the SBC.

2.1 ABC4EU Solution

The solution proposed by the ABC4EU project consists of a two-step segregated ABC system, with a self-enrolment stage that is performed in a kiosk physically separated from the e-door, and a verification stage that is properly performed at the e-door.

2.1.1 Enrolment Stage

In the process of enrolment, the traveller must present his/her eMRTD and his/her biometric features. The system must, on the one hand, contrast the data of this document with the corresponding databases, and on the other hand, certify that the traveller is the true holder of the document. To do so, the system validates the biometric data stored on the document (“chip sample”) with the biometric data captured at that moment (“live enrolment sample”).

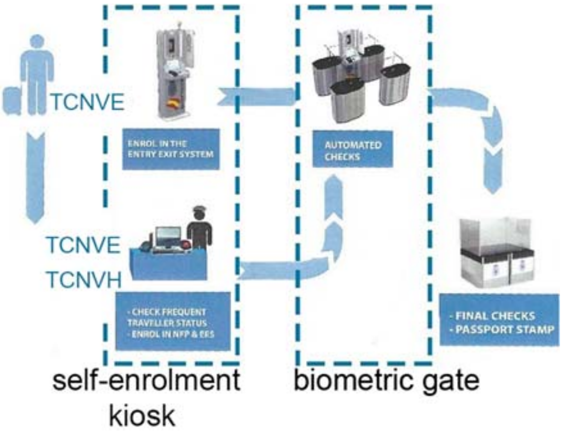

Figure 4: Simple scheme of an ABC4EU system (image owner ABC4EU project).

After registration and when the traveller’s document verification is a success, the system stores the registered traveller’s data for a limited period of time. During this time interval, the traveller can proceed to the e-gate for the verification stage.

Two different protocols have to be applied depending on the type of traveller. On the one hand, TCNVE travellers can do the enrolment at the e-kiosk when arriving at the airport before their trip. In case they are frequent travellers, they can enrol the system only once at their consulate, which allows them to avoid repeating the enrolment in every trip. On the other hand, enrolment at the airport is not available for TCNVH travellers, so they must enrol the system at the consulate before the verification stage at the airport.

2.1.2 Verification Stage

The verification stage consists in comparing a new capture of the traveller’s biometric data (“live check sample”) with the biometric data captured at the selft-enrolment stage (“live enrolment sample”).

The verification process always takes place at the e-door and after the enrolment stage. Both the TCNVE travellers and the TCNVH travellers must pass this stage.

2.2 PAD in the ABC4EU Systems

A presentation attack occurs at the capture phase (sensor level) of the biometric subsystem. As phases: one at the self-enrolment and the other one at the biometric gate, this causes the system to have two vulnerable points to a PA.

To cover all possible scenarios, we shall consider

Table 1: Summary of all possible scenarios in our experimental setup.

	Operation made	Bona fide presentation	Presentation Attack	
Enrolment stage	Document identification	A passenger presents his/her genuine travel document in the expected way	An attacker presents a manipulated travel document (case not considered here)	
	Biometric verification (chip sample vs. live enrolment sample)	A passenger presents his/her genuine biometric features in the expected way	EPA: An attacker tries to cheat the enrolment system with someone else's biometric features, with manipulated biometric features or is not collaborative with the system	EPA + VPA: An attacker cheats the enrolment system with someone else's biometric features, with manipulated biometric features or is not collaborative with the system, and does it succesfully. Then the attacker tries to repeat the attack with the verification system.
Verification stage	Biometric verification (live enrolment sample vs. live check sample)	A passenger presents his/her biometric features in the expected way	VPA: After a bona fide enrolment made by a passenger, an attacker tries to cheat the verification system with someone else's biometric features, with manipulated biometrics features or is not collaborative with the system	

three different presentation attacks:

- Enrolment PA (EPA), when a presentation attack occurs at the self-enrolment stage. For example, an attacker provides the system with documentation that belongs to someone else and therefore tries to impersonate the true holder of the documents.
- Verification PA (VPA), when a presentation attack occurs at the verification stage. An attacker tries to impersonate a traveller who has previously enrolled the system. For example, a correctly registered traveller loses or is stolen his/her documents between the self-stage and the verification stage. Then an attacker uses those documents to try to pass the verification.
- Enrolment and Verification PA (EPA + VPA). In this case, an impersonation has occurred at the enrolment and the attacker continues impersonating the true traveller at the verification stage (double attack). For example, an attacker presents travel documentation that belongs to someone else and gets successfully enrolled. After that, in the verification stage the attacker continues to impersonate the true holder of the documents in order to cross the e-gate.

These three possible scenarios complicate the evaluation of the PAD subsystem (see Table 1).

3 EXPERIMENTAL SETUP

A pilot experience was performed at the Adolfo Suárez Madrid-Barajas Airport T4-S international arrivals terminal in December 2016. This airport, which serves the capital of Spain and the centre of the Iberian peninsula, is the busiest airport in Spain, the fifth one in Europe and the 24th one worldwide regarding passenger traffic. In 2015 it reached an amount of almost 47 million passengers (ACI, 2016).

As we said above, ABC4EU systems capture the fingerprint and an image of the face in the biometric subsystem. Some studies have focused on fingerprint recognition for these types of systems like Donida Labati et al. (2016), but in our experiments, we have focused on facial recognition for two reasons. On the one hand, the face image is the only biometric reference which is compulsorily present in all passports in the world (in the Schengen zone also the fingerprints of the left hand). And on the other hand, the face is a feature that, in case of a false negative system response, an agent can always contrast the information with an easy visual inspection.

With our tests, we have analysed the attacks at the self-enrolment stage (ESA) and at the verification stage (VSA), both in isolation.

For the enrolment, the original passports have always been used and all the PAIs have been built with features of 9 people, who are also the owners of those passports. Thus, a bona fide presentation (chip sample) is cross-matched against one bona fide presentation (enrolment live sample) and against 6 attacks with different PAIs.

At the verification, only those cases where the enrolment has been made with a bona fide presentation are used. In this way, a bona fide presentation (enrolment live sample) is cross-matched against one bona fide presentation (verification live sample) and against 6 attacks with different PAIs.

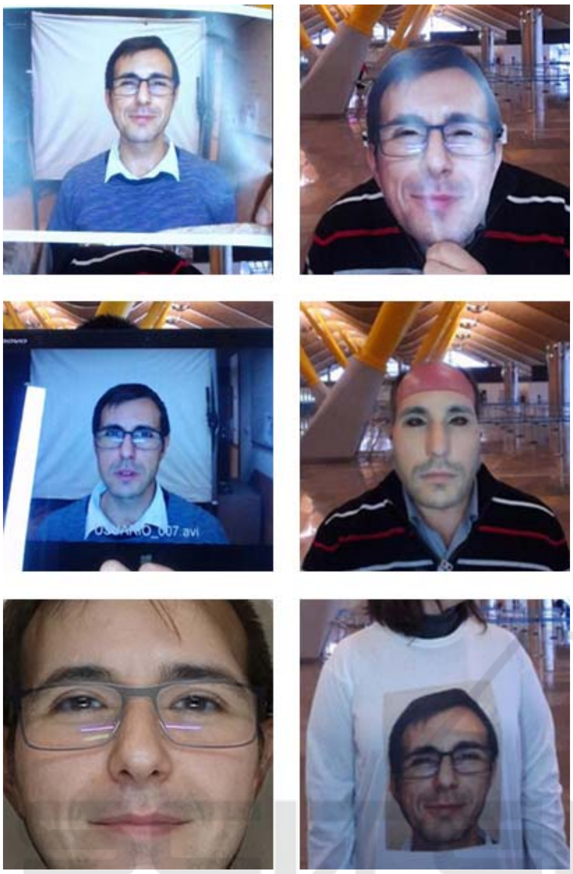

Figure 5: Different PAIs used to test the system. From top to bottom and from left to right: Photo, Mask, Screen, 3D Mask, Morphing, T-shirt.

We have selected several common PAIs found in literature to test our facial PAD system (Figure 5), which are summarized as follows:

1. Photo attack: It consists of presenting a printed photograph of the traveller intended to be impersonated.
2. Mask Attack: It consists of wearing a paper or cardboard mask with the traveller's face. The eyes of the mask are trimmed to avoid blinking-based life detection systems.
3. Screen Attack: It consists of using an electronic device to play a video of the passenger, also to surpass the life detection system.
4. 3D Mask: It consists of using a resin mask, captured and printed with 3D technology. This type of masks allows attacking more sophisticated capture systems using Kinect cameras or 3D scanners (Nesli Erdogmus, 2014).
5. Attack T-Shirt: It consists of wearing a T-shirt on which a photograph of the traveller to be impersonated has been stamped.
6. Morphing Attack: It consists of blending the face of the traveller with the face of the attacker using image fusion software, similarly to the work by Ferrara et al., (2014). However, in our tests the biometric information stored at the passport is never modified. We present a printed morphing image to the capture system.

Our PAD system returns a probability that the presentation is bona fide presentation.

To verify the integrity of the system against the attacks and to analyze the PAD obtained data, several curves have been calculated, like the usual ROC curves, which represent in biometrics the false negative and false positive rates for the different thresholds. In this case the curves present the obtained APCER and the BPCER rates.

Because of security reasons (the pilot was performed in a critical area with a real border crossing), the amount of test subjects was limited. This restriction is the reason of relatively small number of some of the attacks.

Table 2: Amount of presentations to test at the enrolment and verification stages.

Enrolment		Verification	
Bona Fide	16	Bona Fide	18
Photo	9	Photo	4
Mask	9	Mask	5
Screen	5	Screen	6
3D Mask	6	3D Mask	6
Morphing	8	Morphing	7
T-Shirt	7	T-Shirt	2

During the self-enrolment stage, see Table 2, 61 presentations were made with 6 different travellers, taking into account bona fide presentations attempts and attacks with the different PAIs. At the verification stage, 93 presentations were made in total, but we will only use 48, those in which the enrolment was made with a bona fide presentation. We have ignored double attacks (EPA+VPA).

4 RESULTS

In a PAD system, as in most biometric systems, *APCER* errors and *BPCER* errors cannot be considered equally important. As mentioned above, the *APCER* error is considered a measure of system security while the *BPCER* is a measure of the convenience of the system.

In ABC systems, we must consider security as the most important factor against convenience, so it is advisable to set a threshold value that returns a low *APCER* value even if it increases the *BPCER*. Since

ABC systems are controlled by an agent, always a bona fide presentation considered as an attack, in other words a false positive, will trigger an alarm that can be verified and corrected by an agent

In Table 4 we can see *APCER*, *BPCER* and *ACER* values for different thresholds at self-enrolment and verification stages. As we said the decrease of the *APCER* entails an *BPCER* increase, but considering security as our objective, a threshold of 80 at self-enrolment and 95 at biometric gate would be the most suitable. As seen in the table those two thresholds are the ones that have less *ACER* in its stage.

In Figure 5, the graphical representation of *APCER* vs. *BPCER* for all threshold range is presented in the case of self-enrolment stage. The attacks results are presented both: individually for each attack and globally aggregating all attacks. Same information is present in Figure 6 for the gate stage.

In the obtained curve for the self-enrolment stage (Figure 5), it is observed that the most dangerous attacks for the system are the screen attacks and the photos attacks (T-Shirt attack has more *APCER* but this result cannot be generalized because data shortage), while the other attacks like morphing attack are easily detectable in this stage. Although at verification most of the attacks have a higher *APCER* value than in the enrolment, it is morphing attack clearly the one that most succeeds in deceiving the system (Figure 6). This behaviour can be explained observing the difference between the reference image use in the facial verification in both situations. In self-enrolment kiosk, the reference image is the chip passport image, in the case of the e-gate, it is the life image acquired previously in the self-enrolment kiosk.

The low quality of the biometric feature presented in the facial image passport allows a less successful detection morphing attacks than in the case of a more recently life image used in the e-gate.

Also in the results, it is possible to see that for most of the attacks, the *BPCER* in enrolment is higher than in the verification. This indicates that the enrolment system is less friendly and will reject more presentations even if there are bona fide presentations.

In general, the experiments in the enrolment have a lower *EPCER* than the same ones at verification (Table 3). This indicates that the self-enrolment stage is more robust to attacks than the verification stage, i.e. fewer attacks have been classified as bona fide presentations (*APCER*) and fewer bona fide presentations have been classified as attacks (*BPCER*). All this shows that using is biometric passport information to detect attacks, as done in the enrolment (chip sample vs. live enrolment sample), is more reliable than comparing the capture at verification with the capture in the enrolment (live enrolment sample vs. live check sample), two current images of the passenger.

Table 3: *EPCER* (Equal presentation classification error rate) of each of the PAIs in the self-enrolment and verification stages.

PAI	*EPCER* (enrolment)	*EPCER* (verification)
Photo	0.2000	0.2071
Mask	0.0333	0.2071
Screen	0.1505	0.1714
3D Mask	0.0	0.0
Morphing	0.0	0.5000
T-Shirt	0.2583	0.0
All PAIs	0.1210	0.2106

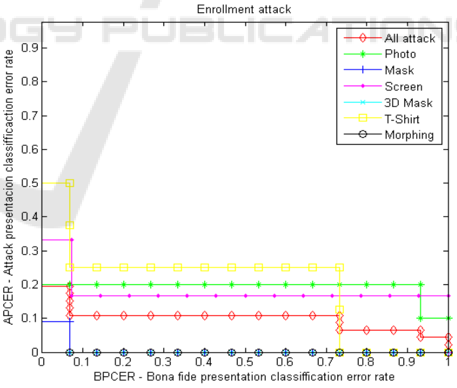

Figure 5: *APCER-BPCER* curve in the self-enrolment stage.

Table 4: *APCER*, *BPCER* and *ACER* values for different thresholds at enrolment and verification.

Self-enrolment					
threshold	**40**	**70**	**80**	**90**	**95**
APCER	0.7609	0.3261	0.1739	0.1087	0.0217
BPCER	0.0	0.0	0.0667	0.7333	1.0
ACER	0.3804	0.1630	0.1203	0.421	0.5217

Biometric gate					
threshold	**40**	**70**	**80**	**90**	**95**
APCER	0.8276	0.6552	0.5862	0.4483	0.2069
BPCER	0.0	0.0	0.0	0.0	0.1429
ACER	0.4138	0.3276	0.2931	0.2241	0.1749

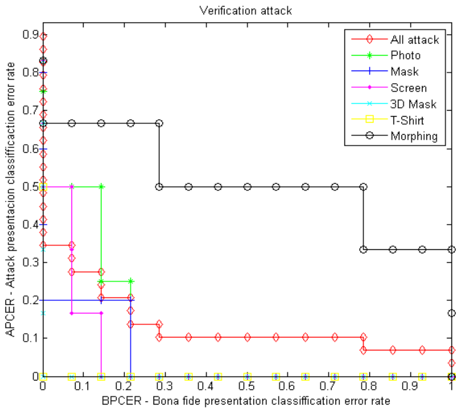

Figure 6: *APCER-BPCER* curve at the verification stage.

The reason for this difference is that the PAIs for the attacks are usually built with more recent passenger photos. For example, in our tests the PAIs were constructed with photos taken a few days before the tests. This means that the differences between the PAI and the passenger appearance are added the differences between the oldest passport image and the current appearance of the passenger.

5 CONCLUSIONS

In this paper, we have presented the results of a pilot experience carried out with a two-step segregated ABC system. This pilot was performed with real ABC e-gate developed in ABC4EU project and in a real border crossing at T4-S terminal of Adolfo Suárez Madrid Barajas Airport in December 2016.

The system comprises two stages that are carried out in two different devices. On the one hand, the self–enrolment kiosk where the passenger is register after the system check out his/her biometric features with the biometric features stored on submitted passport. And on the other hand, the biometric gate where the system verify that the passenger is the same that made the register in the e-kiosk, comparing the biometric features of registered passenger against the biometric feature of the passenger present in the gate.

With our experiments, we have tested the security of the system, especially the capture of the biometric subsystem, testing its response to presentation attacks. We have tested different types of attacks with artefacts commonly used to perform impersonations, such as photos, paper masks, video screens, 3d mask or printed t-shirts.

The results obtained allow us to draw three important conclusions.

First, we can say what attack are the most dangerous for the system and against which of them the surveillance should be increased: Video attack or photo attack in the self-enrolment stage, while in the biometric gate stage morphing attack is the most effective.

Also, we have proposed the optimal thresholds that minimize the average error (*ACER*) in both stages of the system. Those thresholds are different for each one stages, being higher the threshold in biometric gate than in the self-enrolment stage.

And finally, we have realized that the first verification that is carried out in the self-enrolment e-kiosk is safer than the one that is performed in the biometric gate. This is due to the face image in passport is usually lower quality than the captured face image and it is older too. These two factors have important impact in the PAD results and make two things clear: If the PAIs (presentation attack instrument) were constructed with images of the passenger very similar to those of their documents, the verification and enrolment errors would be comparable and the system would be more vulnerable. And also, from the point of view of the system security, in order to increase the detection of attacks, a countermeasure could be that the biometric gate should make two verifications: contrast the captured image of the passenger with his/her image in the self-enrolment and again with the image of the passport.

In the pilot the system security protocols are not yet fully established and the PAD control has not yet been activated. In future tests, the development of the pilot will be more advanced and the system will allow more exhaustive experiments. For example, some future work will be an analysis of different possibilities of cross-match between attacks in the self-enrolment and attacks in the biometric gate. And another future experiment would be to check the results if the PAIs for the attacks were made with same images of the traveller's documents.

ACKNOWLEDGEMENTS

This work has been part of the ABC4EU project and has received funding from the European Union's Seventh Framework Program for research, technological development and demonstration under grant agreement No 312797. This work has been already part of the BIOinPAD project and has received funding from the Spanish Ministry of Economy, Industry and Competitiveness under the reference TIN2016-80644-P.

REFERENCES

ABC4EU, 2014. Automated Border Control Gates for Europe. http://abc4eu.com.

Airports Council International (ACI), 2016. Year to date passenger traffic DEC 2015. http://www.aci.aero/Data-Centre/Monthly-Traffic-Data/Passenger-Summary/Year-to-date.

Berklund, E., Karbauskaite, R., 2008. Frontex perspectives on biometrics for border checks. In *Proceedings of BIOSIG'08*, pp. 107-116.

Boeing, 2016. Current Market Outlook: 2016 – 2035. http://www.boeing.com/resources/boeingdotcom/commerc/about-our-market/assets/downloads/cmo_print_2016_final_updatup.pdf.

Cuesta Cantarero, D., Pérez Herrero, D. A., Martín Méndez, F., 2013. A multi-modal biometric fusión implementation for ABC systems. In *2013 European Intelligence and Security Informatics Conference*.

Donida Labati, R., Genovese, A., Muñoz, E., Piuri, V. Scotti, F., Sforza, G., 2016. Biometric Recognition in Automated Border Control: A Survey. *ACM Computing Surveys*, Vol. 49, No. 2, Article 24.

Erdogmus, N., Marcel, S., 2014. Spoofing Face Recognition With 3D Masks. *IEEE Transactions on information forensics and security*. Vol. 9, No. 7, July 2014, pp. 1084-1097.

FastPass, 2016. FastPass: a harmonized, modular reference system for all European automated border crossing points. https://www.fastpass-project.eu.

Ferrara, M., Franco, A., Maltoni, D., 2014. The Magic Passport. In *2014 IEEE International Joint Conference on Biometrics*.

Frontex, 2012. Best Practice Operational Guidelines for Automated Border Control (ABC) Systems, version 2.0. ISBN 978-92-95033-57-3.

ISO/IEC 30107-1:2016(E), 2016a. Information Technology – Biometric Presentation Attack Detection – Part 1: Framework.

ISO/IEC JTC 1/SC 37 N 6364, 30107-3, 2016b. Information Technology – Biometric Presentation Attack Detection – Part 3: Testing and Reporting (Draft). http://isotc.iso.org/livelink/livelink?func=ll&objId=17578675&objAction=Open&viewType=1.

Kosmerlj, M., Fladsrud, T., Hjelm, E., 2006. Face recognition issues in a border control environment. In *Advances in biometrics Lecture Notes in Computer Science*, Ahang AKJ, D. (ed.), Springer Verlag, pp. 365-372.

Ratha, N. K., J. H. Connell, Bolle, R. M., 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, Vol. 40, no. 3, pp. 614-634.

Sánchez del Río, J., Moctezuma, D., Conde, C., Martín de Diego, I., Cabello, E., 2016. Automated border control e-gates and facial recognition systems. *Computers & Security*, Vol. 62, pp. 49-72.