BIOMETRIC SYSTEM IN AVIATION INDUSTRY (SECOND PART)

A REPÜLÉSIPAR BIOMETRIKUS RENDSZEREI (MÁSODIK RÉSZ)

ALSHAMAILEH Lafee[1] – ŐSZI Arnold[2]

Abstract

This review aims to summarize all applied and hypothesized alternatives of improving the Risk-Based Security (RBS) which are applied by the Transportation Security Administration in order to optimize the unique way for passenger screening and to inspect the present RBS passengers screening platform. It also aims to review current biometric technologies and highlighst current incorporation of biometrics into RBS initiative programs. Several governmental programs, which have combined biometrics into their measures to develop the proficiency and consistency by using biometrically enriched security measures, were investigated. This review will give a insight into how to include biometrics into the current Risk-Based Security Aviation Passenger Screening Program.

Keywords

Aviation Security, biometrics, Transportation Security Administration, Risk Based Security (RBS)

Absztrakt

Ez az áttekintő cikk a gyakorlati és a feltételezett alternatívák összefoglalását célozza meg, amelyek segítik a Veszély Alapú Biztonság (Risk-Based Security, RBS) növelését. Ezt a Transportation Security Administration alkalmazza, páratlan utas vizsgálattal és a jelenlegi RBS utasvizsgáló plattformmal. A cikk áttekinti a jelenlegi biometrikus technológiákat és kiemeli az RBS induló programokba bevont biometriát. Számos kormányzati programot vizsgáltunk, amely a biometriát használja a méréseihez, hogy növelje a hatékonységot és a következetességet. Ez a review cikk egy jó rátekintést ad arra, hogy hogyan vonjuk be a biometriát a jelenegi kockázat alapú repülés biztonsági utas átvizsgáló programba.

Kulcsszavak

Repülés biztonság, biometria, Transportation Security Administration, Kockázat Alapú Biztonság (Risk Based Security, RBS)

[1] lafee.alshamaileh@uni-obuda.hu| ORCID: 0000-0002-5141-4786 | PhD student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] oszi.arnold@bgk.uni-obuda.hu | ORCID: 0000-0001-5988-0143 | adjunct professor/egyetemi adjunktus | Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

ABBREVIATION

US-VISIT: unveiled United States Visitor and Immigrant Status Indicator Technology
DHS: Department of Homeland Security
TSA: Transportation Security Administration
RBS: Risk-Based Security
CAPPS I, II: Computer Assisted Passenger Pre-Screening
IATA: The International Air Transport Association

INTRODUCTION

Biometric technologies play a vital role in the simplification of more appropriate and protected passengers processing systems. Though, these growths are disintegrated. There is a must for information sharing on optimized practices and lessons learned in order to have the augmented configuration.

In recent years, different technologies and applications in biometric technologies have become increasingly widespread, and parallel to this, the subject is also attracted by academicians. The different evaluation of the developed methods depending on their areas of use causes the number of biometric methods to increase. However, these methods' common point is that risks are minimized, and the safest system is established. Another critical issue, which is the main reason for these security concerns, is the operation of these technologies and ensuring their cybersecurity that does not harm people's information security and constitutional freedom. This issue, which every biometric method developed pays attention to, has been frequently questioned in recent years, but the legislative arrangements have not been fully completed yet.

In USA, Transportation Security Administration (TSA) integrates unpredictable security measures, both seen and unseen for high quality service. Combining biometric systems is one of TSA services. TSA is an agency of the U.S. Department of Homeland Security that was created in 2001 to be responsible for passenger security in American air.

Incorporating biometric technology that validates an individual’s identification will mend the competence and efficiency of the screening system since biometrics offers more superior security and accessibility than traditional approaches of personal recognition. Biometrics can replace or enhance the existing technologies.

The idea of the biometric system is that once a passenger match between facial characteristics and the passport is created, the passenger will be able to proceed through all of the terminal checkpoints from the curb to the cabin. In addition, biometric systems will allow the TSA to re-concentrate on high risk or unknown risk travelers thus increasing security effectiveness.

This review will give visions on how biometrics can elevate key features of the passengers processing at airports and it will discuss many new opportunities arising from improved biometric technologies and methods, intelligent use of networked data and sophisticated public/private partnerships.

Biometric innovation is rising as the best arrangement for aircraft and aeroplane terminals to mechanize character checks amid rising traveller numbers. Concurring to Biometrics for Way better Travel: An ID Administration Transformation, a report distributed nowadays by SITA. It traces how utilizing biometrics to check passenger’s character will control quicker and more secure self-service forms at aeroplane terminals as traveller numbers are set to nearly twofold to 7.8 billion by 2036.

Airlines and air terminals are as of now contributing to different shapes of biometric innovation, and SITA's report investigates inventive ID administration programs that are changing the travel encounter nowadays. Within the future, these will be more commonplace around the world as 63% of aeroplane terminals and 43% of carriers arrange to contribute to biometric ID administration arrangements within the following three a long time.

BIOMETRIC SYSTEM AND AIRPORT SECURITY

Air travel has become a standard not only in international travel between countries but even in domestic flights between cities. Reducing air travel costs close to the costs of land travel made air travel preferable to land travel in terms of costs and reducing travel time, which causes airports to become more crowded. Not only citizens but even diplomatic visitors, government officials, foreign and domestic tourists, and immigrants pass through airports to travel from one city to another. This makes airports vulnerable to provocation attempts and terrorist acts and creates security vulnerabilities in them.

Given that terrorism has become a global threat, security weakness cannot be tolerated. However, it is impossible to fill this security gap by increasing the number of security personnel or resources allocated to security. Because of the congestion of airports, security personnel cannot over-pay attention to more than one problem or verify more than one topic simultaneously. There are inevitable gaps and blind spots in such an environment, so airport security must be handed over to flexible and scalable technology and systems.

The People's Republic of China is one of the leading states in this field. China can follow its citizens very closely within the social credit system framework, which was first announced in 2018. This practice, which is considered Orwellian-style social engineering, is also criticized seriously for the violation of private life privacy. The information screens at Chengdu Shuangliu Airport add a different dimension to the use of biometric data. The system provides this information by scanning the face of the passenger and matching it in the database. The most interesting aspect of this practice at Chengdu Shuangliu Airport is that the passenger does not need to have his / her face scanned at any point in the airport as per their request. To put it more clearly, even if the passenger made the check-in process using known methods (check-in counter, kiosk, mobile, internet, etc.), but at the airport but somewhere in the city, the face of the passenger in question was scanned and entered the database of the relevant system. As a result, although there are opponents, it seems that the use of personal data in the electronic environment will become increasingly common. Thus, it seems that the "good" citizens will have a lot easier on their travels.

Several biometric systems were used at different facilities at airports. The following scheme (Figure 9) shows a representation for the possibilities to place a biometric system.

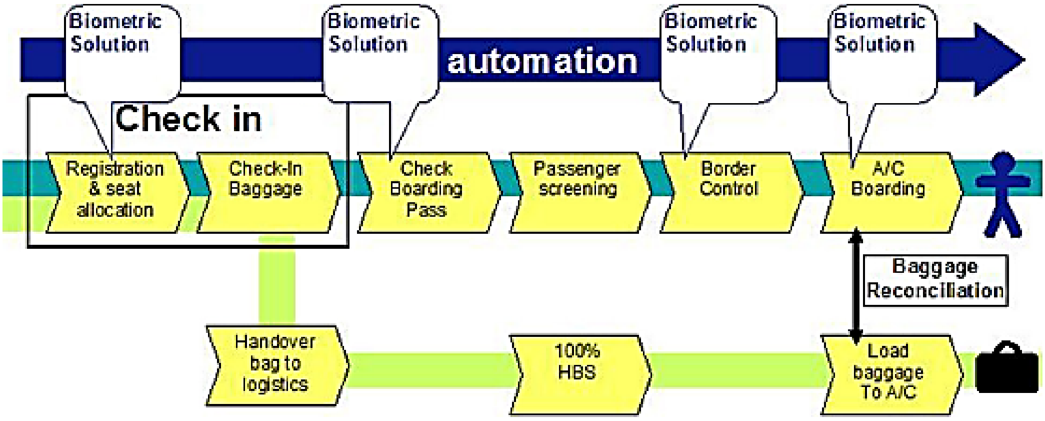

Figure 9: Diagram courtesy of Fraport; based on Simplifying Passenger Travel (SPT) Programme's Ideal Process Flow

The integration of many biometric solutions during passenger processing will smooth the passenger flow through the airport. When practicable, airports and their investors in one location should work with airports and the stakeholders in other locations, to develop interoperable systems that will let a traveler move from one location to another using the same travel token.

Some examples for biometric systems are represented in next section.

CASE STUDIES IN THE USA

In this section some case studies will be discussed showing their system engineering design of biometric systems and decision-making support in complex biometric-based systems.

Ross and Coworker reported in his work the process of a digital biometric measurement, primarily data is collected then it is transformed to set of numbers or codes and then stored in a database. As soon as the database is gathered, it is matched to other measurements previously stored in the database to see if there is a match. [18]

Ever since September 11, 2001, the Department of Homeland Security (DHS) and, within it, the Transportation Security Administration (TSA) has been established by the American federal government, which is responsible for passenger security at the nation's many airports.

A. US-VISIT

As per the unveiled United States Visitor and Immigrant Status Indicator Technology (US-VISIT) and according to the Department of Homeland Security (DHS), new techniques were executed for all the visitors from nominated countries that pass in the United States at different ports of entry to be photographed and fingerprinted by customs officials. [19] As stated by DHS, using the biometric identifiers will provide higher security than the use of name databases alone, particularly since persons will not be able to claim another's identity or fake travel documents. All the stored data will be safely stored, and it is just available only for the authorized and official usage, that international travelers are who they say they are and do not pose a threat to the United States. [19]

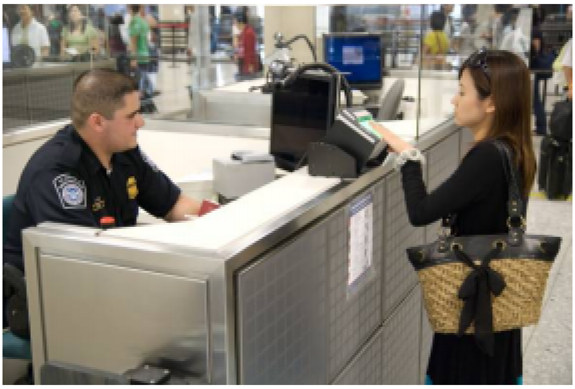

Figure 10: US-VISIT's innovative biometric technology enables officers to efficiently verify

B. CAPPS

The Computer-Assisted Passenger Pre-screening System (often abbreviated as CAPPS) is a counter-terrorism system in place in the United States' air travel industry. The United States Transportation Security Administration (TSA) preserves a watch list of individuals known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety." The list is used to preventively recognize terrorists trying to buy airline tickets or board aircraft traveling in the United States, and to alleviate apparent threats.

There are two versions in the USA of the program called CAPPS. The first version of CAAPS was managed by the FBI and FAA in the late1990s, at that time CAPPS I was implemented in response to the supposed threat of U.S. domestic and international terrorism.

The principle of CAPPS is to screen the selected passengers for additional screening of their checked baggage for explosives. CAPPS selectees did not undergo any additional screening at passenger security checkpoints. [20]

The Office of National Risk Assessment (ONRA) proposed a second version of CAPPS (CAPPS II), with a list of necessities for a replacement to CAPPS I. Some of those requirements were:

- The government, not the airlines, would control and administer the system
- Every ticketed passenger would be screened, not just those who check bags
- Every airline and every airport would be covered by the system

In the summer of 2004, CAPPS II was cancelled by the TSA as the new version of CAPPS II is all dressed up in the language of privacy and concern for freedom, but it fails to address the core problems with the concept and continues to pose an enormous threat to American freedom and privacy.

Shortly thereafter, the TSA announced a successor program, called Secure Flight that would work much the same way as CAPPS II. Secure Flight was implemented in August 2009.

C. Secure Flight

This program matches passenger information against watch lists maintained by the federal government. The initial implementation phase of Secure Flight resulted in the complete transfer of responsibility for passenger watch list matching to TSA from aircraft operators whose flights operate within the United States. The second phase of Secure Flight will result in the transfer of responsibility for passenger watch list matching to TSA for flights into, out of, and over the United States.

The primary differences between Secure Flight and CAPPS II are summarized in Table 1. Unlike CAPPS II, the new system will not seek to identify anyone other than known or suspected terrorists.

Secure Flight Compared to CAPPS II		
Program elements	CAPPS II	Secure Flight
Provides no protection against terrorists with fake IDs	√	√
Provides no meaningful way for individuals to challenge their security designation	√	√
Centers around reliance on secret, inaccurate government terrorrist watch lists		√
Checks personal information against private databases	√	√
Requires collection of personal information from travelers making reservations	√	√
Expands program beyond terrorists	√	
Uses computer algorithms to rate individuals' "threat to aviation"	√	

Table 1: Comparison between CAPPSII and Secure Flight (ACLU Conference) [21]

NEW MODELS FOR AIRPORT SECURITY AND BIOMETRICS

Br¨omme in his article stated that biometric innovation ought to be accessible, for instance with institutionalized information positions for biometric interchanging information, correspondence conventions. Also, it should bring together programming interfaces for empowering the interoperability of various biometric frameworks and parts in existing information and communication technology (ICT) infrastructures. [12]

Improving airport security and immigration pain points with a risk-based approach is a new challenging trend. Smart security does not mean having to wait a long time in a queue, as many companies integrate devices and programs to enhance the airport layout to further improve ambience and passenger flows, e.g IATA/ACI Smart Security program believed to be a catalyst for an important shift in the way certain passengers are screened. [22]

Antoine Rostworowski, Director of Montréal Trudeau International Airport stated that the industry is moving towards this approach where a single token process is feasible, and that could make a difference. IATA, ACI, ICAO and others are having a lot of discussions around this, and biometrics is what many believe is the way forward. [23]

On March 2018, British Airways brough its biometric identification gates to three more US airports. Biometric identification gates were expanded to New York (JFK), Miami (MIA), and Orlando (MCO) airports. These "biometric e-Gates," which have been in trial at Los Angeles International Airport (LAX) since November 2017, use facial recognition to match flyers with their passport, visa, or immigration photos and can remove the need to show a boarding pass or identification when getting on a plane. Lufthansa has started using facial scans to permit passenger self-boarding at Los Angeles International. [24]

Figure 11: Biometrics boom at the airport: Using fingerprints, facial scans to enter clubs, get on planes

CONCLUSION

Any new system must be in line with ACI recommendations, and biometric systems deployed at airports must be compatible with and capable of forwarding data to multiple systems. Systems applicable at airports ought to be fast, efficient, secure, reliable, scalable, certified according to ICAO and ISO standards and conscious of environmental requirements of each location.

Several research and studies must be conducted in cooperation between governments and research centers to optimize the suitable biometric configuration for high level of security which would improve aviation safety in various ways.

REFERENCES

[1] Transportation Security Administration: "49 U.S. Code § 114 - Transportation Security Administration | US Law | LII / Legal Information Institute". Law.cornell.edu. Retrieved 2016-08-08..

[2] Poole, Jr., Robert W. “Airport Security: Time For a New Model.” Policy Study 340. Los Angeles, CA: Reason Foundation, January 2006..

[3] Ross, Prabhakar & Jain, An Introduction to Biometric Recognition, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004, supra note 125.

[4] US-VISIT FACT SHEET, findBiometrics.com, at http://www.findbiometrics.com/Pages/feature%20articles/usvisit.html, 2004.

[5] 2. US-VISIT Data Sheet www.dhs.gov/us-visit.

[6] The Aviation Security System and the 9/11 Attacks - Staff Statement No. 3": "The Aviation Security System and the 9/11 Attacks - Staff Statement No. 3" . 9-11commission.gov. Retrieved 2016-08-08..

[7] ACLU conference, https://www.aclu.org/other/secure-flight-compared-capps-ii.

[8] Eric P. Haas, Back to the Future - The Use of Biometrics, Its Impact of Airport Security, and How This Technology Should Be Governed , Journal of Air Law and Commerce Volume 69 2004..

[9] BIOMETRICS | SECURITY // JUL 2014, Improving airport security and immigration pain points with a risk-based approach, automation and more choice, http://www.futuretravelexperience.com/2014/07/improving-airport-security-immigration-pain-points-risk-based-a.

[10] ACI Media Releases, 2015, http://www.aci.aero/News/Releases/Most-Recent/2015/02/09/Antoine-Rostworowski-joins-ACI-World-as-Director-of-Facilitation-and-IT..

[11] Chris McGinnis, Biometrics boom at the airport,2018, https://www.sfgate.com/chris-mcginnis/article/Delta-other-airlines-bring-biometrics-to-more-12782175.php, Published 11:20 am, Monday, March 26, 2018.

[12] Őszi Arnold, Kovács Tibor: „Theory of the Biometric-based Technology in the field of e-commerce” Óbuda University – CINTI 2011 – 12th IEEE International Symposium on Computational Intelligence and Informatics, 2011. nov. 21-22. ISBN: 978-1-4577.

[13] ACI World Headquarters • Geneva • Switzerland, The Application of Biometrics at Airports, http://www.aci.aero/media/aci/file/free%20docs/aci%20biometric%20position%20final.pdf.

[14] Schneier, “Attack trees,” Dr. Dobb’s Journ. of Softw. Tools, vol. 24, no. 12, 1999..

[15] US-VISIT Program, Increment Privacy Impact Assessment, Dec. 18, 2003.

[16] Bartlow, Nick and Zekster, Gregory. “Holistic Evaluation of Multi-Biometric Systems.” BRTRC, October 2009..

[17] N. G. Leveson, Safeware - System Safety and Computers, Addison-Wesley, 1995.

[18] B. a. I. M. N. S. a. T. C. W. N. 2. National Science and Technology Council. Biometrics in Government Post 9/11. Report.

[19] Svetlana N. Yanushkevich and Anna V. Shmerko ,Fundamentals of Biometric System Design: New Course for Electrical, Computer, and Software Engineering Students, 2009, ISBN: 978-0-7695-3754-2 doi>10.1109/BLISS.2009.27.

[20] Press Release, ACLU, supra note 180..

[21] Center for Army Lessons Learned (CALL). Commander’s Guide to Biometrics in Afghanistan. Vols. 11–25. For Leavenworth, KS: CALL, 2011..

[22] Bundesamt f¨ur Sicherheit in der Informationstechnik (BSI): Vergleichende Untersuchung biometrischer Identifikationssysteme - BioIS, Bonn, Germany, 2000.

[23] Accenture, “Insights into Automated Border Clearance.” Accenture: High performance. Delivered. Chicago, IL: Accenture, 2010.

[24] L. Hong and A. K. Jain, Multimodal Biometrics, in: Jain, Bolle, and Pankanti (eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academic Press, 1999..

[25] National Research Council of the National Academies. Biometric Recognition Challenges and Opportunities. Research Report, Engineering and Physical Sciences, National Academy of Sciences, Washington: National Academy of Sciences, 2010..

Other sources:

https://www.theverge.com/2018/3/9/17100314/british-airways-facial-recognition-boarding-airports

International Journal of Network Security, Vol.2, No.1, PP.52–63, Jan. 2006 (http://isrc.nchu.edu.tw/ijns/)