Information & Security: An International Journal

Alfredo M. Ronchi, vol.39, 2018, xx-yy https://doi.org/10.11610/isij.390x

TAS: TRUST ASSESSMENT SYSTEM

Alfredo M. RONCHI

Abstract: The present paper briefly introduces a general view on tomorrow's border control system and EU inter-BCP real time information sharing, exploring and proposing new operational methods and solutions for border control procedures to increase the efficacy and efficiency of the whole security screening system at the same time reducing the efforts (costs/resources). The general description of the system logic and architecture introduces the core of the solution, the Trust Assessment System. A "black box" based on risk analysis and advanced machine learning algorithms aimed to assign a Traveller Trust Score to each single individual intentioned to cross the border. Main benefits are: improved checkpoint throughput, improved situational awareness and level of security, better traveller experience, optimisation of resources. The concept is that the traveller risk evaluation starts as soon as she/he applies for a visa, a passport or books a trip by whatever means of transport.

Keywords: border security. risk assessment, big data, human factors.

Introduction

As international travel flows continue to rise, there is growing pressure to process large volumes of people and goods at international crossing points without creating bottlenecks; at the same time, with specific reference to the European Union and other federated countries [16], there is a need to provide better security at the "external" borders (land, sea, air), keeping technology costs related to border crossing pointsi as low as possible. Furthermore, the casting of the information net and the reliability of information need to be accurate; moreover, building of trust between parties and the sharing of data are as important as technology advancement. While security cannot be compromised, the traveller's experience should be positive. Trans-border crime causes border instability and vice-versa; hence strengthening border control helps to reduce crime, apprehend terrorists [13] and detect prohibited weapons thus making the inland a safer place. Yet, at the same time, measures need to be appropriate, in terms of efficiencyii, while assuring

i BCP extended control area

ii i.e. large numbers of crossings require quick control checks; maintaining the current level of checks is becoming increasingly expensive

the effectiveness[iii]. In order to achieve such goals, risk-based methods and systems for screening at border crossing must be defined and actually implemented. The use of smart and novel detection technology along with advanced data analytics can truly help to improve detection of potentially dangerous people and goods while limiting to fewer accurate checks informed by pre-selected and preliminary (and non-disruptive) risk-based analysis of the flows, in respect of the quality of life of the traveller, and adding economic vitality to the union of states. The focus of the present contribution is on dynamic multiple source data collection and analysis. The Author of this paper is the team leader of the project and the responsible for the concept and development of the TAS.

Objectives

Today's security screenings concept[iv]: Travellers are all the same, and, thus, bring the same risk; If a visa is not required, there is no pre-screening, so the screening process is entirely performed at the Border Crossing Point (BCP); The screening targets are only the dangerous goods carried by travellers; Human screeners interpret the outcomes of X-ray and ultrasonic scanners[v] and no, or very little, interpretation of both the "historical profile of the traveller" and the human behaviour shown at the BCP is performed; Security screens are concentrated in relatively small, typically congested BCP areas only. More rarely, sniffers (for explosives) and thermo-graphic cameras[vi] are employed to screen travellers and support decision-making. In terms of data sharing[vii], today the European situation is all but harmonised both in terms of data processing and assessment protocols, as well as in terms of Key Security Indicators (KSI) and security resources usage.

Tomorrow security screenings[15]: We must re-think the way technological and human functions are linked. The new human, technological and organisational (HTO) model must be defined based on three innovative pillars: A) Risk-based security screening; B) Security checks typology and, when possible, positioning; C) Real-time and batch networked information sharing.

The screening target will be both smuggling[viii] and the abnormal behaviour of travellers and their estimated intentions. Bona-fide travellers will be quickly separated from the risky ones that will be clustered into virtual homogenous, risk-based groups and processed accordingly. Checks will be performed at different stages in the travel process, from the time the traveller arranges his or her travel

iii i.e. potential threats have to be detected, whereas bona fide crossings should be made smoother or seamless

iv Some relevant projects are: http://www.ewisa-project.eu , http://frontex.europa.eu/intelligence/eurosur/ , https://www.fastpass-project.eu , www.abc4eu.com , http://www.effisec.eu. Last accessed on March 2018

v I.e. what sensors read.

vi As those used with the SARS infection to quarantine monitoring of visitors to a country.

vii E.g. this even between aircarriers companies and airport security operators, passengers registered on destination managers web sites are almost unknown to airport security operators, no information interchange.

viii e.g. concealed weapons, stowaways, illegal substances.

until arrival at his or her destination[ix]. Human functions will directly contribute, with the support of machines and/or animals, in evaluating the traveller's profile, behaviour and intentions.

The primary objective is to provide the border control operators and practitioners with *enhanced situational awareness*, and capabilities to *timely and proper identification of potentially dangerous people and goods*, thus preventing smuggling and human trafficking. This will be achieved through an economically sustainable technological improvement at border crossing points based on risk analysis working on two main levels: customised configuration of BCPs and risk based screening that combines information from multiple sources and can start already when the traveller is planning his or her journey. The integration of information from multiple sources represents an important innovation factor, as the risk assessment will be based on both information provided by the traveller on a voluntary basis (duly checked), agreement with "carriers" and destination managers as well as sensors, PNR[x] [12], EU Entry/Exit system, public social media [18,3], traditional security databases[xi] and other relevant resources[xii] that might provide additional info or weak signal on travellers' movement and intentions.. The key aspects of the solution are:

a) Reduce the cost of technologies in border security applications as a result of risk-based scalable modular border crossing point (MBCP) configuration, and on the shelf low cost technologies;
b) Change border crossing point paradigm from the current "check-everything-at-the-border" to the more efficient "check-everything-till-the-border" (i.e., from a "checkpoint" to a "check-process");
c) Improve security checks from the current "memory-less" approach to a more advanced risk- & memory-based approachxiii;
d) Anchor security checks duration and modes on the amount and timing of information provided;
e) Integrate current physical-inspections-based security checks with contactless or low-invasive detection mechanisms.

The usage of multiple sources of information is motivated by the following reasons: "Official" data, such as PNR or traditional security databases, do not often allow to achieve a whole picture of travellers' movement due to the lack of pieces of information; "Weak signals" on travellers' behaviour, provided by or extracted from additional data sources such as social media and sensors, can complement such a picture to assess the risk profile and perform the so-called "digital

ix e.g. in new "global" approach - even outside airports' perimeters in case of a flying traveller

x Pesonal Name Record http://www.consilium.europa.eu/en/press/press-releases/2015/12/04/eu-passenger-name-record-directive/ Access March 2018

xi E.g. Frontex, Europol, Interpol, FBI, national law enforcement agencies, etc.

xii i.e. dark net, OSINT Open Source Intelligence - https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html Last accessed on March 2018

xiii i.e., based on both historical and current quantity and quality of information provided

screening"[xiv]. The information on travellers' movements[xv] is not enough for assessing the risk level of passengers; we also need information on people behaviour and other attitudes to create an effective (and informed) risk profile to support decisions at the checkpoints. Personal information [17] provided on voluntary basis[xvi] care of travellers, duly checked, may significantly contribute to depict a profile clearing privacy issues. We consider the "additional" information[xvii] according to the "fitness for purpose" approach, taking into account the practicability in collecting them and the "user acceptance". The proposed solution is a system of systems, where multiple sources providing heterogeneous data will be organised, modelled and processed, based on a set of novel data analytics and analysis algorithms. Through adaptive cost-effective solutions for border crossing points and selective checks, the system aims to quickly identify "bona-fide" travellers, thus creating a personal trust profile for each traveller approaching crossing points.

Methodology

In the proposed system perspective, the security check starts the moment a person buys a ticket or applies for a passport or visa (i.e., the earlier the information is provided, the better). In order to enhance security, improve efficiency and reduce costs, we start from four assumptions:

A. Not all borders are equal – maritime and terrestrial perimeters, as well as Northern and Southern perimeters, and/or in other countries Western and Eastern perimeters, require different screening strategies because the people crossing borders and the chorography shaping them are different;
B. Not all travellers and goods bring the same risk. Bona-fide travellers need to feel safe, secure and at ease with the related 'bureaucratic' process. On the other hand, travellers and goods that compromise security and safety should be better detected;
C. The flow of travellers is increasing due to many reasons: tourism, economic migration, political and war refugees;
D. The scarcity of human (and economic) resources to perform security screenings compared to the increasing flow of travellers.

Time management is essential to efficiently perform security checks, thus ensuring an increasing need of higher throughput. The outcomes of the foreseen methodology will range from a light check for bona-fide travellers to a in depth-check or denial to access for risky travellers. In order to create tomorrow's security

xiv The "digital screening" (which also includes the analysis of social media, but also the analysis of other sources in Internet) is an interesting trend that is being pursued also by US (actually they already started with automatic tools). See this article: https://www.forbes.com/sites/kalevleetaru/2017/01/29/we-already-screen-cell-phones-at-the-border-will-social-media-be-any-different/#450fe3a25fa3 Last accessed on March 2018

xv National border In-Out record keeping

xvi Privacy issues are relevant in the activation of this section of the procedure, anyway the "Informed consent" approach can be positively adopted.

xvii which could also include personal information

screenings, we must re-think the way technological and human functions are linked. We will create a new human, technological and organisational (HTO) model with three innovative pillars: 1) Risk-based security screening [4,5]; 2) Security checks typology and, when possible, positioning; 3)Real-time and batch networked information sharing.

One of the key innovation factor is a double tier risk-based approach. On the top level the dynamic Modular Border Crossing Point (MBCP)[xviii] risk-based approach takes into account the first assumption "NOT all borders are equal" in the specific field of typical risks related to the single BCP[xix] optimising the use of resources. On the second level - TAS[xx] - the approach proposes a mix of technological and human functions to identify the "level of trust" characterising each traveller, a score plus some "instructions" about how to interpret the score will represent the output of the "black box" we call TAS. For the purposes of this document we term "sensor" any "module" providing a normalised input to the TAS, that means we consider as input a wide range of data coming from personal information voluntarily provided by travellers to CBRN detectors. Each BCP is configured accordingly with the local needs; this means a potentially different arrangement of "sensors", each active sensor will transfer on the system hub a rich set of normalised data[xxi], TAS will receive such normalised data including historical data coming from the Dashboard[xxii] and process them thanks to the harmonious balance of technology and human factors [14] to identify a Traveller Trust Score[xxiii]. The TTS will provide the basis for each traveller screening and will be broadcasted on the Dashboard. In the proposed HTO model, the risk level of a traveller will determine, for every journey, the screening groups into which the traveller will fall for security clearance. The risk level of a passenger will depend upon three elements, namely:

- The level of information (i.e. amount and quality) provided directly or indirectly by the traveller (or the traveller-related organisation) to the authority mainly before and even during her/his journey;
- The behaviour manifested by the traveller every time s/he travels;
- The nature and characteristics of the travel and previous travelsxxiv.

xviii The configuration of the BCP will be updated accordingly with the foreseen needs.

xix e.g. human trafficking, radioactive substances trafficking, etc.

xx Trust Assessment System - the adoption of a risk-based decision-making process will allow to "process" travellers according to five risk-based groups, namely: Very high-risk passengers (those with a negative security record & negatively signalled by authorities); High risk passengers (those with a negative security record but not signalled by authorities); Medium risk passengers (those with no security record and not signalled by authorities); Low risk (those with positive security record); Very low risk passengers (those with a positive security record and positively signalled by authorities).

xxi sensor data plus annotations, these data will contribute to better interpret raw data provided by sensors and enable the evaluation of human factors

xxii The dashboard connects clustered BCPs and provide access to the system data base and LEA's criminal data banks.

xxiii TAS output includes both TTS score & some "instructions" to correctly interpret the TTS underlining the combined use of tech. and human resources.

xxiv Which countries s/he use to visit e.g. typical touristic locations or blacklisted countries.

In our vision, a traveller, despite being virtually clustered in the low risk category, will be "declassified" to a higher risk category randomly or whenever s/he manifests an unusual behaviour at border screenings[xxv].

Technology Description[xxvi]

The Trust Assessment System is the heart of the entire platform. Despite its inner complexity its functionality is well defined and quite straightforward to understand: main functionality of the TAS module is to compute the so-called "Traveller Trust Score" (TTS). This score is a synoptic index directly correlated to the potential risk induced by each traveller. TTS is calculated using both historical and live data streams gathered via TAS's input channels. TAS is therefore in charge of:

- Gathering data from data sources (Modular BCP, FastTrack APPxxvii, databases, social networks and other sources);
- Running analytics on gathered data to assign a TTS to travellers and thus spot potential threats;
- Serving request originated by the Dashboard or other connected devices;
- Sending notifications when suspects, or potentially dangerous situations, are detected.

Each Modular BCP is configured with the optimised combination of devices/sensors accordingly to the analysis of the specific information (location, risks, geopolitical issues, news, season, etc.). Each "sensor" is managed as a plug-in on the platform and is characterised by some attributes (typology, reliability, etc.) in addition each "sensor" is almost independent from the others (loosely coupled devices).

TAS is based on latest research on big data [18] technology and A.I. algorithms duly merged with human factor analysis [8,14]. From a logical perspective, the TAS is structured as follows: *Data broker layer:* Receive data from data sources and prepare them to be further processed; *Speed layer:* Processes live data streams with low latency; *Batch layer:* Processes large quantities of data with high accuracy; *Serving layer:* Serves data in response to queries, serving either pre-computed views or generating them on-the-fly; *Query engine:* In charge to manage queries execution; *Machine Learning module:* In charge to learn from data and actually calculate TTS.

The TAS's algorithms analyse travellers' behaviour by using: Public data harvested from social media platforms; Data originated from online booking companies for both hotels and means of transportation; Visa applications; Data originated by Modular BCPs; Historical traveller's data. *On the conceptual side*, main activities are: definition of specific protocols, tools and initiatives able to promote and prime travellers' collaboration; creation of a travel tickets on-line registering service; set up of tools and policies to enable voluntary provision of personal information;

xxv the same may happen randomly and in the case of "bona-fide" newcomer profiles

xxvi At a high level of abstraction can be decomposed in the following modules: European Modular Border Crossing Point (EMC); Trust Assessment System (TAS); European Security Dashboard (ESD); EU-FastTrack - web & APP.

xxvii This APP will be accessible to registered users and collects personal information in order to offer a Fast Track to the traveller.

creation of specific informed consent and non-disclosure policies; assuring data privacy. *On the software side*, main activities are: defining interoperability standards of existent databases; defining mechanisms able to securely grant concurrent access to existent public and non-public databases; integration of multimodal biometric [1,9,10] algorithms[xxviii]; use of high performance big data processors and extensive data mining procedures to be applied on web based content (web, Twitter, Facebook, Instagram, etc.); defining optimal dataset describing travellers' history and behaviour.

Data tier is in charge to maintain historical data about travellers, goods, MBCP status (more in general HTO resources), logs and alerts. Is logically viewed as a single resource (i.e. a single database) although in practice is composed by a *Data access layer* which is in charge to mediate access to various data sources, both structured and unstructured, and the *Data sources* themselves. The main source of data is indeed represented by the TAS system although other data sources could be accessed if needed [11].

Logic tier is in charge to mediate access between the Data tier and the Presentation layer.

Presentation layer technically speaking is a RIA (Rich Internet Application) suitable for both desktop and mobile environments. It is implemented using a reliable event-driven framework suitable to implement modern, responsive and effective interfaces.

The integration of the different sources of data will represent the basis for advanced analysis. Given the expected large size of this integrated information a number of Data Science techniques[xxix], including machine learning, deep learning plus artificial intelligence and analytical engine advanced behavioural algorithms will be implemented.

Machine learning technologies will address unstructured data content analytics on one side and time-series / geo-time-series on the other side. The focus of big data analytics will be predictive modelling, based on machine learning techniques, while the focus of security behavioural analytics will be on predictive modelling focusing on traveller's online behavioural characteristics and patterns. Available open source machine learning algorithms will be the starting point for the development of predictive models embedding those algorithms within a more complex software architecture pre-processing the data before the execution of the algorithm and generating and selecting the features representing the input of the predictive model.

xxviii Enhanced biometric unit – full fingers, iris and face (ICAO specifications, AFIS, IAFIS, NGI, IDENT, HART)

xxix Semantic & Machine Learning algorithms engine for data processing and analytics. The implementation of a semantic engine based on Expert System COGITO technology with avant-garde natural language processing (NLP) heuristics combined with Machine Learning algorithms in order to enable the automatic analysis of the data received by the crawler; develop the abovementioned semantic engine by creating taxonomies, ontologies and semantic rules to support specific end users requirements on "border crossing" domain related topics. The development of these rules will be finalized to provide the capability to support automatic content categorization and extraction of key information like entities (people, organization, places), absolute and relative temporal references and relationships among entities; develop a dedicated set of normalization rules to be integrated in the semantic engine, in order to categorize and classify content according to a unified language commonly understood by the European end users in border security domain (achieving a "sharing environment").

The architecture will consider three autonomous databases: *ID:* it will identify individual people including personal data considered as static data, it is the only database that identify individual people; *UNS:* it will potentially able to collect and analyse all unstructured data: texts, social media, emails …, it does not create any personal data-store; *GTS:* it will gather all information collected along the time from all potential source of information, all events will be stored by using "time + geolocation". The separation of these three databases is critical regarding security and privacy issues. Each of these databases will not in situation to present any risk to be used individually. Only authorized applications will be able to: make a connection between the events and the ID of people; access personal data and take profit of global historic datasets generated by an extensive range of data sources and analytics tools. The real big technological move that characterizes the big data revolution is the switch from row-oriented databases to column-oriented databases (more relevant for analytical/OLAP workloads). TAS is going to manage a large range of sources of events including constraints of real time by taking into account large historic datasets.

Big data and social media - an objective of the project is to selectively collect and analyse data coming from different sources including: Social media information (time, location when available, networks, content/semantic); Traditional structured data from institutional databases (ERP …); Travel process events (visa applications, tickets …); ID checks; Sensors data … The traveller's data would generally be collected from publicly available sources or will be provided voluntarily by the passenger to gain access to the "Fast-Track"; private information will not be collected without informed consent, in respect of privacy and confidentiality. This integration represents a major challenge of social media analytics, as insights from the semantic processing and analysis of social media information are tightly bound to the ability of identifying the author of posts and tie his/her activity on social media with historical data from more traditional sources.

The semantic engine part of the solution will be in charge of deep semantic text analysis. This analysis will start from the output of OSINT crawler (either Surface or Deep/Dark Web) or from other kind of sensors acquiring unstructured contents (also web form filled by traveller). If this content will be a multimedia one, a Speech to Text technology (STT) is needed in order to transcribe audio into electronically and accessible text. Understanding events/intentions in advance (Ex-Ante) and apply reasoning to the lessons learned (Ex-Post) are a crucial point from the investigation and deduction point of view. Prevention is the first step useful to understand if someone is writing/telling "bad" words regarding a politician of a country, a critical infrastructure, an organization. At the same time analysing the information coming from historical use cases, so after the event occurred, can give added value either to the live analysing or to the prevention one.

As already mentioned this solution will implement also a crawling for both Surface and Deep/Dark web, to complement and integrate the other sources of information already described previously. The surface crawling component will be based on

open technologies[xxx] allowing end users to set the sources they need to acquire data from. The surface crawler engine will be able to gather content from open sources like RSS, Social Networks (Twitter, Facebook), Web and Search Engines (mainly Google, Bing and Yahoo). Surface crawler will be then extended to Deep Web by integrating additional and dedicated crawlers for these types of sources and combining the overall solution with anonymizers to access Dark Web. Plain text will be then extracted from the original content acquired by the sources under crawling and delivered to the semantic engine, for elaboration (content categorization, entity/relation/emotions extraction, stylometric analysis, etc.). The Deep Web crawler will be based on the adoption and integration of multiple dedicated crawlers, both proprietary and open, in order to have a synergy of their best functionalities and capabilities[xxxi]. In order to extend this capability also to Dark Web, making it even more relevant for illegal activities monitoring, an integration of dedicated proxy solution will be required: TOR and I2P will be mainly considered for this purpose. The fundamental concept is to achieve speed and mobility during the stop and search routine of travellers in every physical location they are. The solution can be used as well for accessing the data of the travellers prior to the date of the planned travel adding value to the TRUST Assessment and delineating a picture of the traveller prior to his arrival to the departure gate.

Developments

<<For the traveller it would be ideal to cross borders without being slowed down. It is indeed likely that, in the next ten years or so, technologies make it possible to implement "no gate crossing point solutions"…>> [European Commission Study]

Recent years have witnessed technological and social changes appearing at an unexpected pace and spanning a wide set of aspects, such as technologies for personal identification, detection systems, social habits, new threats and new privacy and personal (ethical and social) issues. As a consequence, the challenge is to foresee technological solutions and social behaviours ten years from now, and the adoption of different technologies and behavioural models from those in play now. In the transport domain, a trade-off will emerge between the need to guarantee security of travellers, even against unexpected threats, and speed of security controls. Accordingly, it would be ideal for the traveller to be able to cross borders without being slowed down by queuing at crossing points gates as it was experimented in Dubai. The risk-based solution described above represents a sounding a building block to achieve the result. In a decadexxxii from now, technologies will make it possible to implement "no gate crossing point

xxx E.g. Apache Nutch and Apache Camel

xxxi i.e. some of them are particularly efficient with sites requiring user and password, others allow to create customizable crawl models/templates

xxxii PROTECT H2020 project: http://projectprotect.eu/ FRONTEX organizes workshops on Biometrics on the move for gateless BCPs.

solutionsxxxiii" that based on risk assessment methods, allow for seamless crossing of borders and security checks for the vast majority of travellers who meet the conditions of entry, and make sure that those who do not fulfil such conditions are refused entry.

Main aspects to be considered: to understand how these technologies will be accepted (or rejected) by the public and key stakeholdersxxxiv requires greater insight into: (1) the likely constellations of technologies; (2) their potential ethical, legal and societal impacts, and (3) real-world, contextualised acceptability experiments assessing the passenger's "feeling of safety".

Results

This solution aims to apply technologies in an efficient but effective manner by integrating new technologies with a risk-based outcome focussed approach to increase the reliability of the border crossing process and at the same time the experience of the traveller. This solution has been conceived as a system level goal-oriented project, which means that the impact relies on the capacity of the system to integrate in a sound architecture for individual technologies that will provide a larger benefit as a whole than in individual deployment.

The primary objective of the project is to make an economically sustainable technological improvement in security at crossing points based on a risk analysis [2] that combines information from multiple sources to enhance situational awareness for border control practitioners. The technology component is deployed based upon a researched operational concept for risk analysis. Flow management innovation (fair and fast) through innovative multiple information processing and use of advanced sensors / input channels to identify the TTS. Integrate current physical-inspection-based security checks with contactless or non-obvious detection mechanisms (like border physical checks) – progressive migration from actual solutions to the new approach, from the current "check-everything-at-the-border" to the more efficient "check-everything-till-the-border" (i.e., from a "checkpoint" to a "check-process"), from the current "memory-less" approach to a more advanced risk-based approach (i.e. based on both historical and current quantity and quality of information provided).

Business Benefits

The underlying concept is that not all borders crossing points are equal and particular situations and events could change substantially operational conditions, so potentially each BCP could be tailored to suit the needs of an environment at a given time saving unnecessary resources. Thanks to the full implementation of the solution the BCP will improve its throughput without the need to add more

xxxiii *Refer also to the IATA and ACI Smart Security Initiative http://www.iata.org/whatwedo/security/Pages/smart-security.aspx*

xxxiv Air companies, Shipping companies, Railroad companies, Bus companies, Airports, Harbours, Highways companies, Destination managers,, Tourism operators, IATA, EDA, Frontex, Interpol, Europol, etc.

personnel. Use of on the shelf technologies as needed by the specific crossing point and situation.

Economic benefits will derive by reinforcing the effectiveness of crossing borders through approved techniques and procedures this should be seen as an encouragement and reassurance to travel, thus increasing the GDP collectively across and through the countries. Additional benefits are: Ensure privacy and human rights are respected within new approaches to risk-based border crossing; Decrease border crossing times for the majority of travellers; Significantly reduce the cost of border security checks as a result of risk-based scalable border crossing point (BCP) configuration, and on-the-shelf, low-cost technologies. In addition the availability of TAS "sensors" open standards may offer a business opportunity to hard and soft companies.

Conclusions

This paper proposes a new approach to border security checks based on risk analysis and trust assessments shared at the international level, it applies a "harmonisation by design" principle to ensure the progressive harmonisation and homogeneity of the procedures. The key technologies foreseen have been already tested on different borders both in Europe and South America / Africa. The system platform acts on six lines: Innovative double tier risk-based approach to security checks; High-penetration safe technologies for remote and flexible on-the-go screening of persons and vehicles; Mobile solutions based on mass market devices; Travellers' pre-registration; real-time information sharing, traveller's trust profile. "Bona Fide" travellers will benefit from simplified security controls based on prior processing of travel and relevant Internet data. The solution proposes a risk-based, outcome-focused approach to security controls rather than the current "one size fits all" scheme - pre-evaluating a personal risk profile on the basis of the traveller's "history", integrating available international police data, API[xxxv] and PNR data, and public data available on line, within the legal capacity of border authorities. The paper focus on one of the innovative solutions the Trust Assessment System – TAS, a kind of "black box" receiving as input a specific set of data coming from "sensors" analysing traveller's information and behaviour and evaluating a traveller trust score (TTS) that together with additional "instructions" will determine the classification of the specific traveller and consequently the required security check procedure.

References

[1.] Biggio, Battista, et al., "Security evaluation of biometric authentication systems under real spoofing attacks", IET biometrics, Vol. 1, No. 1, 2012, pp. 11-24.

[2.] Cano, J., Rios Insua, D., Tedeschi, A., Turhan, U. (2014), Security Economics: A Multi-objective Adversarial Risk Analysis Approach to Airport Protection, Annals of Operations Research (ANOR),

xxxv Advance Passenger Information

[3.] Ceri Stefano, Bozzon Alessandro, Brambilla Marco, det al.: Web Information Retrieval. Data-centric systems and applications, Springer 2013, ISBN 978-3-642-39313-6, pp. I-XIV, 1-284
[4.] Colombo Simone, "Risk-based Decision Making in Complex Systems: the ALBA Method", IEEE Conference on Industrial Engineering and Engineering Management (IEEM), Bali, Indonesia, 2016,
[5.] Colombo Simone and Golzio L., "The Plant Simulator as viable means to prevent and manage risk through competencies management: Experiment results", Safety Science, Volume 84, 2016, pagg. 46–56.
[6.] Colombo Simone, Nazir S., Gallace A., Manca D., "Experiment-based decision making in complex systems", Chemical Engineering Transactions, Volume 36, 2014, pagg. 85-90, ISBN: 19749791.
[7.] Daugman, J., "How iris recognition works", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, 2004, pp. 21-30.
[8.] Di Giacomo V., Felici M., Meduri V., Presenza D., Riccucci C., Tedeschi A. (2008), Using Security and Dependability Patterns for Reaction Processes, Proceedings DEXA 2008, September 2008, Turin, Italy
[9.] Iris Challenge Evaluation (ICE) http://www.nist.gov/itl/iad/ig/ice.cfm
[10.] Lenharo, S., "Brazilian National Biometric Selection", International Joint Conference on Biometrics, 2014.
[11.] Mtsweni Jabu, Shozi Nobubele Angel, Matenche Kgwadi, Mutemwa Muyowa, Mkhonto Njabulo, van Vuuren Joey Jansen. 2016. Development of a Semantic-enabled Cybersecurity Threat Intelligence Sharing Model. proceedings ICCWS2016, Boston, USA, May 2016. ISBN: ISBN:978191081083-5
[12.] PNR Directive was approved in April 2016 and published in the Official Journal of the EU on 4 May 2016 – see Directive (Eu) 2016/681 of The European Parliament and of The Council of 27 April 2016
[13.] Pollini, A., Tedeschi, A., Cano, J. (2013), Modeling an Emerging Terrorist Threat against Airport Security Scenario, EUROInform Conference, Rome, July 2013.
[14.] Ronchi A.M., Human Factors: feeling safe, Proceedings ICCC 2017, The International Journal on Cyberlaw, Cybercrime and Cybersecurity, New Delhi
[15.] Ronchi A.M., Improving Border Check Point Security, Proceedings ICCC 2017, The International Journal on Cyberlaw, Cybercrime and Cybersecurity, New Delhi
[16.] Ronchi A.M., ICTs for Safety & Security: Their potential relevant impact in the African continent, ISBN 978-1-905824-57-1, IEEE Explore - IIMC International Information Management Corporation, 2017
[17.] Alfredo A.M., Data: ownership, use, abuse and misuse, ISBN 978-93-5254-019-8, The International Journal on Cyberlaw, Cybercrime and Cybersecurity Volume 1 Issue 1

[18.] Shozi NA & Mtsweni J.. 2016. Big data privacy and security: A systematic analysis of current and future challenges. In the proceedings of the ICCWS2016, Boston, USA, p.296-303. 17-18 May 2016. ISBN:978191081083-5

EUROSUR http://frontex.europa.eu/intelligence/eurosur/ ABC4EU - www.abc4eu.com
EFFISEC - http://www.effisec.eu Fast Pass - https://www.fastpass-project.eu

About the author

Alfredo M. Ronchi – expert/advisor in e-Services, General Secretary of the EC-MEDICI Framework of Cooperation and active member of the WSIS since 2003. Head of the JRC Safety, Security, Defence, and Disaster recovery and management. Mr Ronchi is member of the following Boards of Directors: Global Forum, World Summit Award, European Youth Award, European Education New Society Association, Fondazione Italiana Nuove Comunicazioni. Member of the Keio University NoE. Ronchi is appointed as an expert: European Commission, Council of Europe, Italian Association of Banks, National Research Council. He cooperated as organiser or programme chair in W3C, ACM, IEEE conferences. Author/contributor of more than 350 papers and various books on: e-Culture, IPR, e-Government, e-Health, e-Learning, e-Services. Mr. Ronchi is a professor at Politecnico di Milano.