Proceedings of the 2009 Winter Simulation Conference
M. D. Rossetti, R. R. Hill, B. Johansson, A. Dunkin and R. G. Ingalls, eds.

RISK MODELING AND SIMULATION OF AIRPORT PASSENGER DEPARTURES PROCESS

Pravir K. Chawdhry

Institute for the Protection and Security of the Citizen
Joint Research Centre – European Commission
Ispra (VA) 21027 ITALY

ABSTRACT

Airport security is a key element of Homeland Security strategy. This paper presents a process based approach to modeling and simulation of airport security. A quantitative measure of process security, called *permeability*, has been defined. We use the Simplifying Passenger Travel (SPT) model of passenger departures process to illustrate the methodology. Monte Carlo simulation has been used for the departure process to determine passenger process permeability of large airport hubs in a system of interconnected airports. We show the relative impact of the Registered Traveler scheme on improving the security of the passenger departure process. The proposed approach would allow decision makers (a) to identify weakest links in a security chain; (b) to assess quantitatively the impact of deploying specific security technologies on the overall process security; and (c) to help choose the optimum technical solutions to achieve the security goals for a given process in an operational environment.

1 INTRODUCTION

Airport security is a key element of Homeland Security strategy in Europe and the United States. While established line of work on aviation safety has continued to improve the reliability and safety from engineering point of view, new security threats have emerged in the past decades. A worldwide response has been to tighten the security at airports, particularly in the passenger stream. Passengers are now restricted from carrying various everyday items such as water. New technologies for the detection of liquids, gels, explosives and weapons have been introduced, scanning both baggage and passengers. Proper identification of passengers has become mandatory and there too new technologies such as biometrics are becoming common place with the introduction of biometric passports and id cards (BiomCons 2009). The side effect of these initiatives is an increase in operational cost, delays and inconvenience to a large majority of harmless passengers.

While new security measures are introduced, a basic question is often asked: do all the new security measures really make the aircraft more secure, and if so how much more? In other words, *what is the value of a set of security measures and technologies in overall airport security*? Current approaches to airport security means introducing lots of screening and anonymously field testing their effectiveness using the so called Red Teams. This kind of testing is ad hoc, expensive and time consuming while the airport authorities gain little in terms of benchmarking the effectiveness of their security plans.

Airport operators have long benefitted from simulation tools in facility design and operational planning. Several well known simulation packages are now routinely used by most major airports (ARC 2009, SIMCORE 2009). With such tools, planning teams can do *what-if* analysis for various scenarios, configurations and solutions. However, consideration of security in airport simulation tools is limited to the operational impact of security controls rather than their effectiveness. The reason could be that (a) as a business, airports are driven by operational priorities: capacity utilization and resource management, and (b) there is a general lack of security models for airports.

To address the issue of security models, we use a process based approach where security is designed in the process itself, where all the events and transactions take place that may potentially impact security. The security objective then becomes that of ensuring the *integrity* and *availability* of the process, its activities and its actors.

It is well known in the security community that a security chain is only as strong as its weakest link. In the airport security context, what are these security chains? We can recognize them as operational processes embedded with security controls. For example, the passenger process where various checks and controls are made as the passenger proceeds towards the gate. Recognizing that no security system is perfect, we use a probabilistic model for the security of airport passenger departure process based on Simplifying Passenger Travel (SPT) Ideal Process Flow (SPT 2006). Then we define a security metric (called *permeability*) of the end-to-end SPT process. This gives an objective measure of assessing the effectiveness of various

links in our security chain. Airport security violation can be considered as an instance of *rare events*, where there is a very small probability of a breach to occur but the consequence of it can be catastrophic (Rubino and Tuffin 2009). Therefore we use Monte Carlo technique in our security process simulation. We apply it to a large airport hub where the security performance is assessed for mainstream passengers alongside a dedicated stream of Registered Travelers of low risk profile. We also evaluate the security of transit passenger stream. With the motivation to enable benchmarking of airport security nationally and internationally, we do simulation on a network of airports where permeability of transit passenger streams incoming to the hub is assessed under the assumption that the airports implement similar security procedures differently leading to a diverse security performance, that we attempt to measure here.

The rest of the paper is organized as follows. In Section 2, we describe related work on airport security modeling. Section 3 describes the airport departure process with a brief overview of the SPT ideal process flow and the Registered Traveler Scheme. Section 4 describes the airport process security where we develop the airport security requirements and the security of the Ideal process flow. We then develop a security metric for the passenger departure process. Section 5 presents the Monte Carlo simulation of the departure process for ideal process flow where results are given for the permeability of the departure process with and without RT at a large European airport. Simulation results for the process permeability in a network of airport hubs are also presented. Finally, in Section 6we present the conclusions of this research.

2 RELATED WORK

Main approaches to airport security modeling can be categorized as: formal models, passenger flow modeling, security threat modeling, and security checkpoint optimization, as shown in Figure 1.

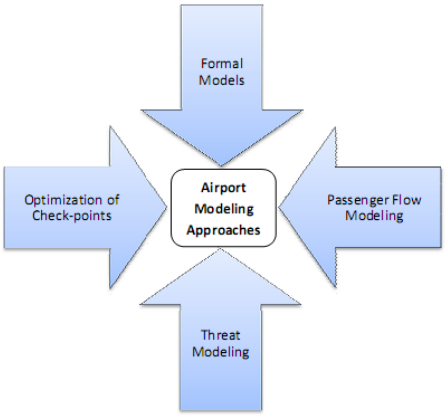


Figure 1: Approaches to Airport Security Modeling

In EDEMOI project, Ledru *et al* have developed formal models of airport security based on natural language description of airport security requirements stated in international standards and regulations (Ledru 2005). They used a graphical notation based on UML to derive their models. The objective was to deploy verifiable models for the certification of airport security procedures. The idea is that semi-formal and formal models can provide an automated procedure for consistency checking of security requirements and their implementation. The initial scope of EDEMOI was on the landside, focusing on the passenger departure process.

Xie *et al*. carried out safety and capacity analysis for terminal airport approach (Xie, Shortle, and Donohue 2004). They developed an agent-based model of approaching aircraft, taking into account their trajectories during approach to runway. A reduced safe separation distance was calculated using the model to help improve the landing capacity. They defined performance metrics for capacity and safety aspects. Airborne delay and runway landing rates were used for capacity, and simultaneous runway occupancy probability for safety.

Early work on the simulation of passenger security system was reported by Pendergraft *et al.* (Penergraft, Robertson, and Shrader 2004). The authors applied the business process re-engineering approach to the passenger process. Their simulation models were built for demand modeling and capacity analysis of *as-is* and *to-be* processes. Results were presented for passengers arrival pattern over a week at BWI Pier C. The methodology was used to provide analytical support for operational policy development of the airport.

Focus at the US DHS on airport security was reflected in the development of simulation tools such as SCO – Security Checkpoint Optimizer (Wilson, Roe, and So 2006). SCO aims to provide planning and operational support by inter-related evaluation of the impact of new or modified airport procedures and facilities on the security effectiveness, operational costs

and passenger throughput. A number of commercial simulation tools already exist for airport design and planning support but they do not explicitly evaluate the security impact (ARC 2009, SIMCORE 2009). SCO uses the usual constructs in its model such as entities, traverse elements, properties, filters and resources. The authors show the impact of checkpoint procedural changes on performance forecast: queue length and waiting times as well as utilization and throughput. Although the original aim was to show security effectiveness, no related results were presented. In a subsequent development of NetSCO, the plan was to extend visualization with a Web interface and to add more complex passenger behaviors.

More recent work in this field includes the idea of dynamic security in an airport terminal (Weiss 2008) which uses an agent-based model to simulate interaction between the passengers and the security system, both represented as software agents. ExtendSim software tool was used to defined the agents and their behavioral functions.

3 THE AIRPORT DEPARTURE PROCESS

3.1 SPT Ideal Process Flow / Passenger Process Model = The SPT Process / Ideal Process Flow

SPT is an IATA initiated program in partnership with airports, airlines, government authorities, ground handlers and technology suppliers (Gupta and Davidson 2007). The aim is to simplify passenger travel by streamlining and automation of passenger processes for air travel while addressing related security concerns.

SPT has defined the Ideal Process Flow (SPT 2006) as a basis for its stakeholders to achieve the above aim. The IPF outlines an ideal view of passenger processing in air travel on the medium term (5-10 year horizon). It presents a detailed view of departure, arrival and transfer processes including the interactions between activities of the airline, the passenger, government authorities and baggage handler. The IPF aims to leverage on current technologies and international standards to achieve the objective of a connected journey. Figure 2 shows a high-level abstraction of the IPF departure process from the passenger's perspective. The detailed process model can be seen in SPT:IPF specification (SPT 2006).

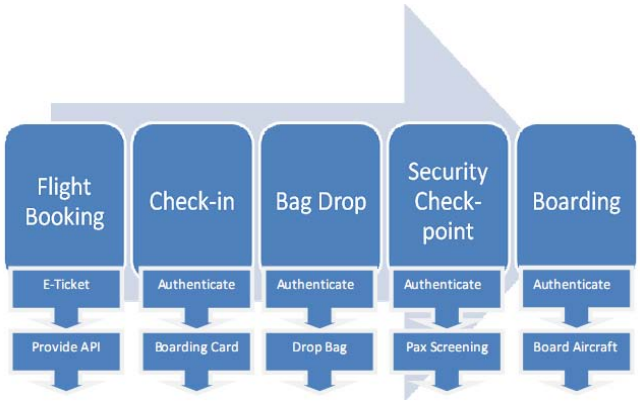
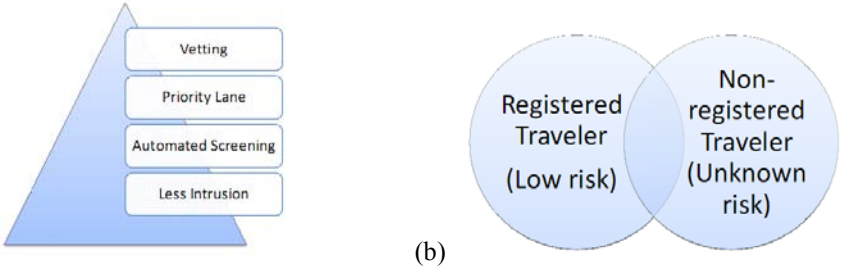


Figure 2: High-level abstraction of the Ideal Process Flow Departures Process (Passenger's view)

3.2 Registered Traveler Scheme

The motivation behind Registered Traveler or Trusted Traveler schemes is a combination of needs for increased border security alongside fluent travel facilitation for bona fide passengers. The underlying principle of RT scheme is to separate potential travelers into low-risk and high-risk passengers, as shown in Figure 3.



(a) (b)

Figure 3: (a) Key aspects of Registered Traveler (RT) Paradigm; (b) Risk classification in RT

The low risk status is accorded based on the security vetting and previous travel history of a person. Once admitted to the scheme, the low-risk status remains valid for a fixed period (say, 2-3 years) during which the scheme member can benefit from facilitated security checks and border control in automated self-service lanes.

One of the necessary conditions for a RT scheme to work as intended is that only the entitled members are able to take the benefit of the scheme. Therefore it should be virtually impossible for a non-member to use a genuine RT credential issued to someone else. This problem has been resolved by the use of biometric identification of all scheme members. Table 1 shows a few examples of RT schemes in operation or run as pilots in recent years, along with the types of biometrics used. An overview of European RT schemes is given in (Frontex 2008). Figure 4 shows how RT scheme may use the SPT model for automated processing of low risk passengers, though current RT schemes only use a small part of SPT process.

Table 1: Examples of Registered Traveler Schemes

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

* No separate enrolment is required

\# The scheme uses EU biometric passport as reference token

RoW = Rest of World; EU = European Union; NZ=New Zealand

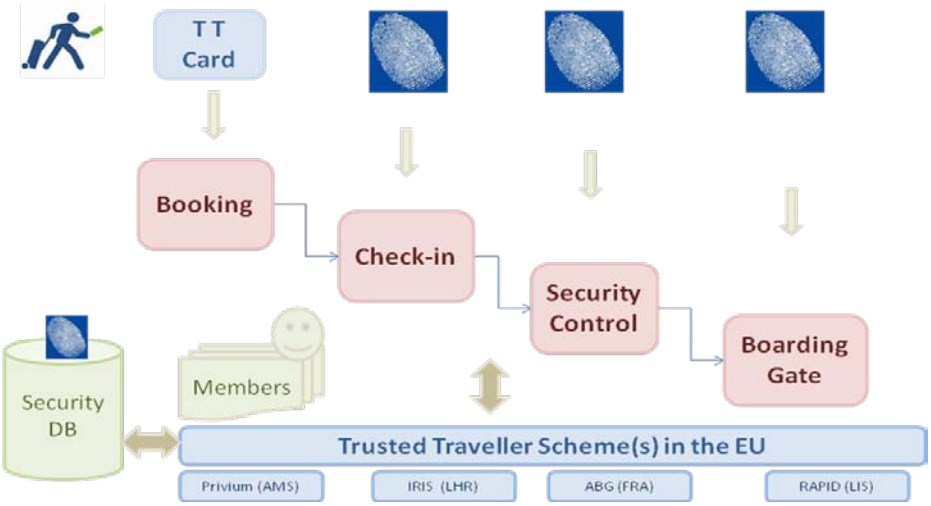


Figure 4: Biometric Identity – Glue between Ideal Process and Registered Traveller

4 AIRPORT PROCESS SECURITY

4.1 Secure airport concept

Security at airports is generally treated as an infrastructure issue and a lot of effort is put into designing perimeter security and various checkpoints. Although useful by itself, it only presents a static picture of airport security. However, due to complex operational make up of airport activities that take place over a period of time, the dynamics of airport security also needs to be understood. Therefore we have taken the *system-oriented* approach to airport security.

Our concept of a secure airport views an airport is complex *system* and security is one of its *states* which changes with time as various processes are executed by a large number of actors and events. For security as a state to be controllable, it needs to be modeled and either measured or estimated in terms of the airport process parameters. Once the observed or estimated values of the security state are known, they can be compared with the target values (set points) and appropriate control action can be taken in real time or periodically, depending on the type of model is developed.

We propose to model the dynamics of airport security around the concept of its *processes*. A thorough analysis of the overall airport security would therefore require good quality process models covering all its operations. It is reasonable to say that explicit modeling of airport processes and associated security metrics would allow us to do systematic simulation studies.

We take the hierarchical approach to developing security requirements. At the high level, one can say that the overall security goal of the airport is to eliminate threats to its aircraft (on ground, in vicinity). Next we look at the various processes that interface with an aircraft. The security goal now is to ensure that each of these processes is secure. Next we look at the activities and agents in the processes and ensure that they are all secure.

To explain how this approach works, within the scope of this paper we focus on a key process: the *passenger departures* process.

4.2 Security of the Ideal Process Flow

Security in the Ideal Process Flow is treated implicitly rather than explicitly. Whereas an information system perspective of security has three formal security requirements: confidentiality, integrity and availability (HMSO 2005), the process perspective of security is somewhat broader and formally less developed.

For process-based security, we take a workflow based approach to process management. Specifically, in the passenger process we propose that a passenger may be viewed as a *workflow item* of the departure or arrival process. For simplicity, we exclude the baggage handling tasks. For the security of these processes, therefore each workflow *item* must be handled in a formally secure manner. Moreover, the workflow implementation should satisfy the information systems integrity criteria. The instantiation of a workflow item occurs with the flight booking activity *i.e.* when a person becomes a booked passenger.

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

The use of biometric identification in border control and registered traveler schemes is a means for fulfilling the requirement of strong authentication of a person's identity. It should be recognized that establishing the true identity of a passenger is only a part of the security process and, by itself, is not sufficient to fulfill the security requirements of the passenger process. Various threats to the process should be taken into account to satisfy its security objectives.

We quantify security of the passenger process through a risk model. The risk is defined in terms of an aggregate of underlying vulnerabilities, threats and impact. For the passenger process, some of the vulnerabilities are as follows:

i) Booking: use of stolen credit card; use of stolen/synthetic identity;
ii) Check-in: use of stolen/synthetic identity; check-in dangerous bags;
iii) Security check-point: use of stolen/synthetic identity; use of stolen boarding card; import harmful substances; import disabling equipment
iv) Boarding: use of stolen/synthetic identity; use of stolen boarding card; import harmful substances; import disabling equipment
v) On-board: use of violence; attempt to hijack; attempt to set off explosion; attempt to disable the aircraft systems electronically.

4.3 A Quantitative Measure of Passenger Process Security

The security of the passenger process is (in part) a function of the following explicit criteria:

(i) the effectiveness of detection of harmful substances that could eventually pass through to the aircraft;
(ii) the effectiveness of identification of malicious persons who could eventually board the aircraft.

Based on the above criteria, we introduce a security metric called *permeability*, for the passenger process. However we acknowledge that there would be additional security metrics for the passenger process, to embody properties such as availability and other aspects of process integrity emerging from the information systems perspective.

Definition 1 "Permeability is defined as a statistical measure of the *residual inability* of the combined procedures and technologies in the process to successfully filter out *all threats* (harmful substances and malicious persons) from reaching an aircraft through the passenger process."

We apply the above definition to the passenger departure process. Consider the SPT ideal process flow in which departure process $\mathbf{P_d}$ is composed of a network of activities $\mathbf{A_i}$. For simplicity, we consider the following sequence: *booking*, *check-in*, *security screening* and *boarding*. We define the effectiveness of the security detection and screening at each activity stage A_i as $P(A_i)$ the probability of successfully filtering out the malicious substance or person. Table 2 shows the stage-wise elimination of threats as well as residuals.

Table 2: Threat Detection and Net Leakage in the Simplified Departure Process P_d

	Effectiveness		
SPT Departure Process stages	**Probability of detection at the stage**	**Threat Detection**	**Leakage**
Booking	$P(A_1)$	$P(A_1)$	$1- P(A_1)$
Check-in	$P(A_2)$	$P(A_2).(1- P(A_1))$	$(1- P(A_1)).(1- P(A_2))$
Security checkpoint	$P(A_3)$	$P(A_3).(1- P(A_1)).(1- P(A_2))$	$(1- P(A_1)).(1- P(A_2)).(1- P(A_3))$
Boarding	$P(A_4)$	$P(A_4).(1- P(A_1)).(1- P(A_2)).(1- P(A_3))$	$(1- P(A_1)).(1- P(A_2)).(1- P(A_3)).(1- P(A_4))$
Full Process $\mathbf{P_d}$	$P(\mathbf{P_d})$	$1 - \prod (1- P(A_i))$, $i = 1,.. 4.$	$\prod (1- P(A_i))$, $i = 1,.. 4.$

The process *permeability*, defined in terms of the *residual inability* of the sequence of all activity stages in the simplified process $\mathbf{P_d}$ to successfully filter out threats, is therefore equal to the *net leakage* shown in Table 2:

$$P(\mathbf{P_d}) = \prod (1- P(A_i)) , \text{ where } i = 1, \ldots 4.$$

The above probabilities for each stage may be determined through laboratory testing of technical equipment, parameterized for various sensitivity thresholds, and through empirical trials of human-centered processes (Wilson, Rose, and So 2006).

The formulation for permeability would be more complex for the full version of the ideal process flow where checked baggage screening and other forms of passenger screening measures are anticipated.

The aim of deploying security technologies in the passenger process is to eliminate identifiable threats. Detection of harmful substances relies on the screening of checked-in bags and hand bags, and passenger's body scan. Identification of malicious persons is based on the intelligence data, genuineness of identity and determining the intent – this last one being the greatest challenge at present for technology developers. As the technologies for detection, identification, intent mature, we can expect an overall improvement in the process security. Furthermore the processes may be redesigned to improve operational efficiency and security. Nevertheless, evaluation of the overall process effectiveness requires simulation, which is the subject of the next section.

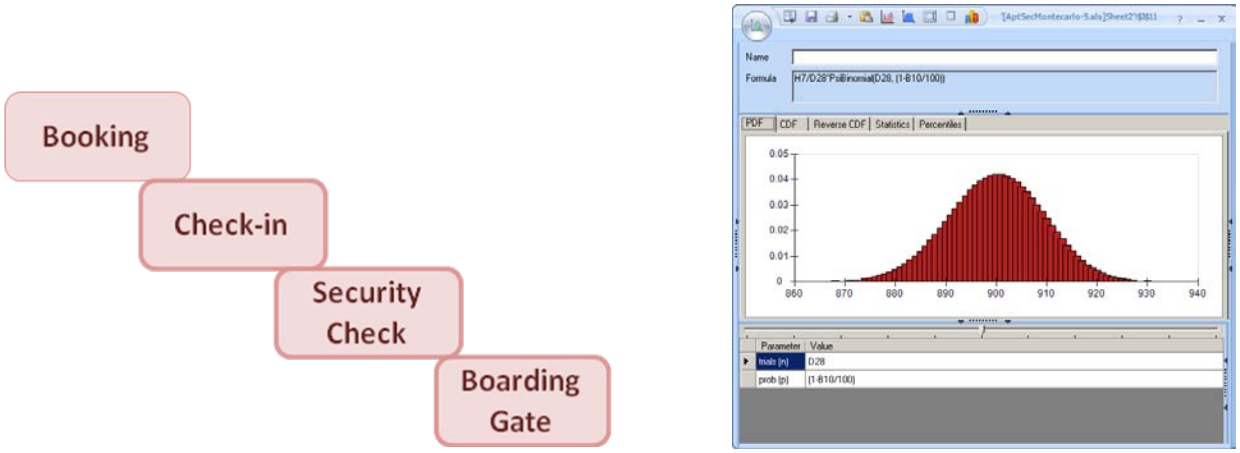
5 MONTE CARLO SIMULATION

5.1 Simulation Setup

Large airport hubs carry tens of millions of passengers every year. By deploying a set of technologies the authorities hope to ensure that the process security is as tight as possible. However, they lack evidence of how effective the systems are altogeth-

er. Use of Red Teams is the main approach to test the systems in blind field tests. However, Red Teams are expensive and the methodology does not provide statistically speaking, a sufficiently large and representative sample. Besides doing *what-if* analysis is not always possible with this approach.

Considering the fact that we are dealing with very large numbers of initial passengers, and the probability of the cumulative failure in detection, though very small but a failure to detect could have catastrophic effect on the flight security, we chose to carry out Monte Carlo simulation of the passenger process, while applying our security metric, defined in the previous section. See (Raychaudhuri 2008) for an introduction to Monte Carlo simulation. The simulation was carried out in Excel using Risk Solver Engine (Frontline 2009).



(a) (b)

Figure 5: Monte Carlo simulation of the departure process; (a) Four stages of the departure process; (b) Binomial PDF with varying probability of detection assumed at each stage.

5.1.1 Scenario 1: Regular Passenger Stream

Initially, the process was defined as shown in Figure 5(a), with different probabilities of detection at each stage as shown. The probability values for each stage were taken as an educated guess. Binomial probability distribution function, as shown in Figure 5(b), was assumed for all stages in the simulation, due to a lack of exact test data in real life. It was assumed that a malicious person might make several attempts to get through, trying to deceive the detection system. The whole process was run on an average daily traffic of 149041 passengers (54.4 million/year), representing a major European airport. The MC simulation had a repeat run of 1000 cycles.

5.1.2 Scenario 2: Registered Traveler Stream

The simulation set up was modified to include two streams of passengers going through the same process, enacted in parallel. One stream consisted of the regular passengers, whereas the other stream consisted of the members of a Registered Travelers scheme where every applicant is vetted for security and background check. To compare the effectiveness of security systems in the two streams, we assumed a 50-50 split of the passenger traffic (as it would reach on a future date with the success of various RT Programs). The effectiveness of the screening systems was assumed to be identical for the two streams.

5.1.3 Scenario 3: Transit Passenger Stream

The next scenario was to include transfer passengers, arriving from a trusted airport, who had to receive a boarding card for the connection flight. The transit passengers had to go through the check-in, security control and gate control like all other passengers. A split of 40-40-20 per cent was assumed between the three passenger stream: regular, RT and transit. Again, the effectiveness of corresponding screening systems in the three streams was assumed to be identical.

5.1.4 Scenario 4: Airport hub in a network of airports

This scenario was created to analyze the role of transit passengers on the security of a major hub. Traffic load at four major European hubs was considered along with varying percentage share of transit passengers in the rage of 20% - 70%. For simplicity, we assumed that each hub was fed by transit passengers from eight regional airports. The split of transit passengers coming from regional airports was chosen randomly.

In this scenario, we assumed that there existed a national baseline for airport security control etc in each country. The national hub and its regional feeders were however allowed individually to use higher standards than the national baseline. The simulation studied the effect of varying security standards in the airport hub network. The same approach was applied to all four national hub-feeder networks.

Simulation results for the four scenarios are presented next.

5.2 Simulation Results

5.2.1 Scenarios 1 and 2: Mainstream and Regular Passenger Stream

Simulation scenario 1 is a subset of scenario 2. Therefore we describe scenario 2 results here. Starting with a net daily passenger flow of 149041 per day, two passenger streams were created with an equal share. The two passenger streams are shown by the two trees in Figure 6. The tree on the left represents processing of mainstream passengers, and the one on the right corresponds to RT passengers.

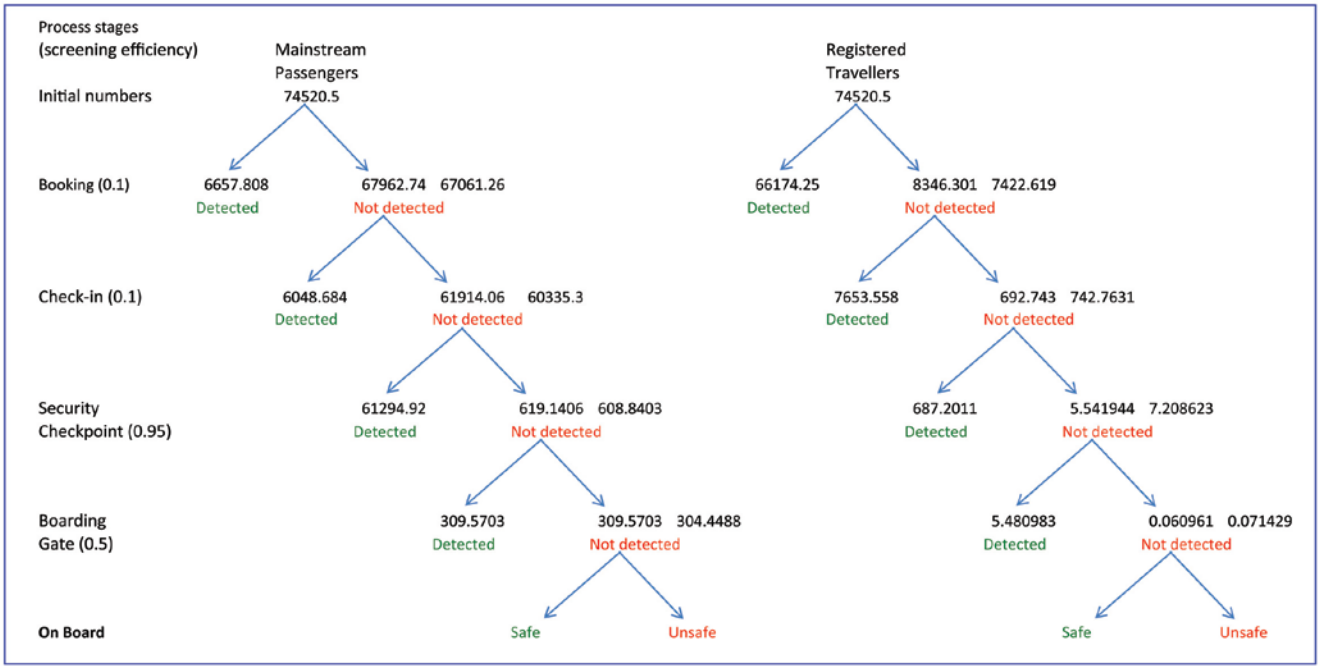


Figure 6. A Monte Carlo simulation run for Mainstream and Registered Traveller Stream for a large airport, showing number of passengers correctly screened (detected) at each stage of the process. The process stages are shown in a column on the left, including corresponding screening efficiency in parenthesis. The simulation is based on a daily passenger flow of 149041, equivalent to 54.4 million per year.

For both streams, the effectiveness of detecting suspicious cases for each stage is shown in the left-hand column. At each node in the tree, the correctly detected cases were flagged, and are shown in green. The undetected cases were allowed to go through unflagged, hence shown in red. These nodes represent the vulnerability of the passenger screening system For the mainstream, under the assumed efficiency of various stages, whereas a very large majority was correctly screened at least once, it turns out that a significant minority of about 304 among 74520 passengers each day would still go through onboard without being correctly screened at any stage of the departure process at all. In other words the security process failed completely for 304 cases *each day*. This was essentially the result of Scenario 1 based on half the daily numbers. At every red

node, there are two figures: one resulting from a specific simulation cycle (on the left hand side) and the other averaging over 1000 cycles (on the right hand side). The difference between the two numbers represents the deviation between an individual run and the average over 1000 cycles. The average figure represents the Monte Carlo simulation result. The behavior of the onboard passengers though categorized under the labels *safe* and *unsafe*, could not be quantified due to lack of a model.

Now let us consider the right hand stream in Figure 6, the one for Registered Travelers (RT). Efficiency of the vetting process in the RT scheme was assumed to be 90%. Therefore the RT passengers stream was considerably sanitized (hence, low risk) even before the first stage (flight booking). To allow meaningful comparison of the RT versus mainstream, The RT passengers were subjected to the same quality of security controls in the departure process as the mainstream passengers. The end result was that of the initial 74520 RT passengers, almost none (0.07) went on board with complete non-detection.

5.2.2 Scenario 3: Inclusion of Transit Passenger Stream

In this scenario, a third stream was created to represent transit passenger. The absolute numbers of originating Mainstream and RT passengers were kept at the same level as in Scenario 2. The transit stream was therefore effectively an added passenger load on the airport. The share of total number of passengers was assumed to be: Mainstream originating 40%, RT originating 40% and Transit 20%. The Transit passengers were passed again through the same controls as the originating passengers. It was assumed that the advanced passenger information (API) was used on arriving transit passengers even before issuing them with onward boarding cards.

Figure 7 shows the graph of undetected passengers in the three steams, plotted on a $\log_{10}$ scale, for each of the stages in the passenger process. Starting with roughly the same numbers, the three streams had markedly different overall security performance in terms of process *permeability*. In particular, permeability for the RT and Transit streams was at a highly desirable level (below -1, equivalent to less than 0.1 passenger). Use of API in the Transit stream was found to be as effective as the vetting procedure of the RT scheme.

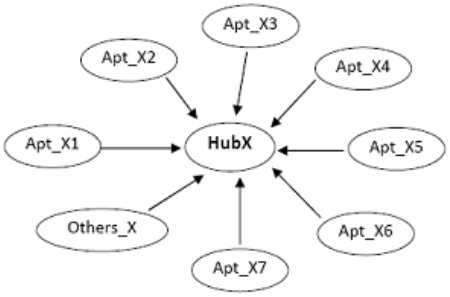
Figure 7. Permeability of the Passenger Process. The graph shows number of pax undetected at each stage on logarithmic (base 10) scale. Process stages are: 1=starting numbers; 2=booking (for mainstream and RT); 2= API screening (for transit passengers), 3=check-in; 4=security checkpoint; 5=gate. Simulation was based on a daily load of 213000 passengers.

5.2.3 Scenario 4: Network of Airports

In this scenario, we studied the effect of variations in security control standards across airports within a country as well as across different countries. We assumed four national hubs, each being fed from its regional network of feeder airports. This scenario was described in Section 5.1.4.

Figure 8 shows the effect of threat propagation and control in a simple hub network. Specifically, it shows the effect of using a security level higher than the national baseline in terms of varying permeability. A major hub ***HubX*** is taken where baseline efficiencies for detection during ticketing, check-in, security screening and gate control are assumed to be 0.1, 0.1,

0.95, and 0.5 respectively (Figure 8, row 3). We assume that the feeder airports have adopted new technologies and procedures to enhance the baseline efficiency by a further 10-70% (column 3) over and above the baseline for security screening and boarding gate. This leads to a significant variation in daily permeability rate within a network of airports, as shown in the last column of Figure 8. By knowing the quality of security process at feeder airports, specific measures may be implemented at arrival gates on a selected basis to ensure that the transit passengers are screened in an optimal way.



HubX Transfer Feed	
Source	*Numbers*
Apt_X1	1000000
Apt_X2	1000000
Apt_X3	1000000
Apt_X4	1000000
Apt_X5	1000000
Apt_X6	1000000
Apt_X7	1000000
Others_X	7000000
Total Feed	14000000
Orig PAX	54400000
Total PAX	68400000

(20% of 68.4M/yr)	Number of Undetected Passengers					
	Ticketing	*Check-in*	*SecScrn*	*Boarding*	*MeanVal*	*Per day*
Baseline Eff.	0.1	0.1	0.95	0.5		
0.3	935000	833085	23326.38	8537.455	9879.294	27.06656
0.7	909000	819918	11478.85	1549.645	1808.161	4.953867
0.1	905000	812690	34132.98	15325.71	16323.54	44.72202
0.4	896000	799232	21579.26	6193.249	7319.345	20.053
0.2	896000	817152	35137.54	14476.66	12974.14	35.54558
0.3	891000	801900	27264.6	9297.229	9878.878	27.06542
0.2	903000	804573	34596.64	14738.17	12828.24	35.14588
0.2	6314000	5669972	238138.8	95731.81	90955.83	249.1941
	12649000	11358522	425655.1	165849.9	161967.4	443.7464
	48979258	44073196	445912.1	223035.3	223035.3	611.0557
	61628258	55431718	871567.2	388885.2	385002.7	1054.802

Figure 8. Threat propagation in a network of airports (Hub-regional network).

The effect of regional variations is shown graphically in Figure 9, for four hubs, each with seven feeder airports. Graphs show the number of undetected transit passengers per day from each feeder airport; identical annual traffic of 1 million transit passengers is assumed coming from each feeder.

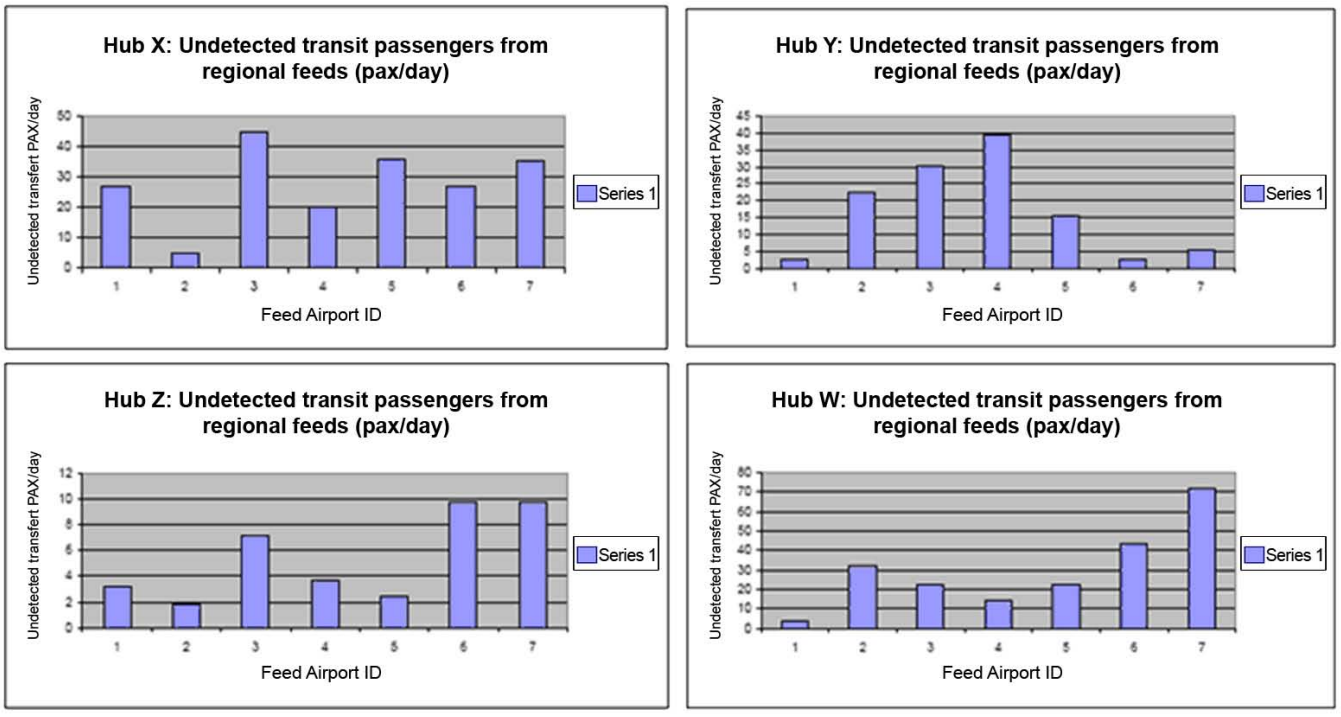


Figure 9. Possible regional variations in the permeability of transit streams at four hubs due to specific security measures in different feeder airports.

6 CONCLUSIONS

Airport security continues to be a key element of homeland security. Even though various national and international security regulations exist, their application varies widely across the airports. When new security technologies are deployed, their impact on enhancing airport security needs to be assessed objectively. A quantitative measure for the security is therefore required.

This paper has presented a process based concept for measuring the security of the passenger process. The security measure is called *process permeability*. We simulated the passenger departure process in four scenarios, ranging from a single airport to a network of hub-regional airports. We also quantified the effect of schemes such as Registered Traveler and Advanced Passenger Information System in improving the security of the passenger process. Simulation of the passenger process was based on Monte Carlo technique.

The aim of deploying security technologies in the passenger process is to eliminate identifiable threats. Detection of harmful substances relies on the screening of checked-in bags and hand bags, and passenger's body scan. Identification of malicious persons is based on the intelligence data, genuineness of identity and determining the intent – this last one being the greatest challenge at present for technology developers. As the technologies for detection, identification and behavior monitoring mature, we can expect a measurable improvement in the overall process security. Furthermore the processes may be redesigned to improve operational efficiency and security. Process simulation and use of objective metrics for security will help decision makers to arrive at the best evaluated options in a complex and ever changing operational environment of airports.

In this context, the Mitre Corp. approach to airport security is relevant. It is based on attack-defense (action/response) strategy and uses a multi-layer model to counter the attack vectors from terrorists (Anderegg 2007). However its theoretical dimension needs to be developed further since current approach seems to be pragmatic: based on creating likely scenarios and identifying all possible attack vectors. A theoretical process-based model, like the one proposed in this paper, might help to anticipate possible attack vectors and thereby identify the security requirements systematically.

7 ACKNOWLEDGMENT

This work was carried out under the exploratory research project on airport security, funded by an IPSC Exploratory Research Grant in 2008.The author would like to thank the IPSC Scientific Committee for their support, and to his colleagues in the research project for useful discussions.

REFERENCES

Anderegg, A. 2007. Risk model for dynamic aviation security. Technical Presentation Mitre Corporation. Available <http://www.mitre.org/news/events/tech07/3088.pdf> [accessed August 26, 2009].

ARC 2009. CAST Passenger Terminal Simulation v. 1.8. Airport Research Centre GMBH. Available via <http://www.airport-consultants.com/index.php?option=com_content&view=article&id=26&Itemid=51> [accessed August 26, 2009].

BiomCons 2009. Introduction to biometrics. The Biometrics Consortium. Available via <http://www.biometrics.org/introduction.php> [accessed August 26, 2009].

Frontex 2008. BIOPASS, study on automated biometric crossing systems for registered passenger at four European airports. Frontex Technical Report, ISBN 978-92-95033-00-9.

Frontline 2009. Risk Solver Engine software. Frontline Systems. Available via <http://www.solver.com/rse.htm> [accessed August 26, 2009].

Gupta, A. and R. Davidson. 2007. Simplifying passenger travel (SPT) program. In *Third symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards*, Montreal, October 2007. Available via http://www.icao.int/mrtdsymposium/2007/Docs/W4_GuptaArun_DavidsonRobertt.pdf [accessed August 26, 2009].

HMSO 2005. BS7799-3:2005. Information security management systems - guidelines for information security risk management, Her Majesty's Stationary Office, UK. Available via <http://17799.standardsdirect.org/bs7799.htm> [accessed August 26, 2009].

ICAO 2008. Simplifying passenger travel's ideal process flow (IPF). International Civil Aviation Organization Working Paper FALP/5-WP/6 (28/02/08). Available via <http://www.icao.int/icao/en/atb/sgm/fal/falp/Docs/wp06_en.pdf> [accessed August 26, 2009].

Ledru, Y., M. Lemoine, D. Bert, V. Donzeau-Gouge, C. Dubois, R. Laleau, F. Peureux, and S. Vignes. 2005. Modeling Airport Security: the EDEMOI approach. Available via <http://vasco.imag.fr/EDEMOI/PresentationsPubliques/ModelingAirportSecurity.pdf> [accessed August 26, 2009].

Pendergraft, D. R., C.V. Robertson, and S. Shrader. 2004. Simulation of an airport passenger security system. In *Proceedings of the 2004 Winter Simulation Conference*, eds. R .G. Ingalls, M. D. Rossetti, J. S. Smith, and B. A. Peters, 874-878. Available via <http://www.informs-sim.org/wsc04papers/110.pdf> [accessed August 26, 2009].

Raychaudhuri, S. 2008. Introduction to Monte Carlo simulation. In *Proceedings of the 2008 Winter Simulation Conference*, eds. S. J. Mason, R. R. Hill, L. Mönch, O. Rose, T. Jefferson, J. W. Fowler, 91-100. Available via < http://www.informs-sim.org/wsc08papers/012.pdf> [accessed August 26, 2009].

Romano, E. 2005. Airport risk assessment. Technical Report Department of Transportation Engineering, University of Naples. Available via < http://sed.siiv.scelta.com/bari2005/143.pdf> [accessed August 26, 2009].

Rubino, G. and B. Tuffin (eds). 2009. Rare event simulation using Monte Carlo methods. Wiley. ISBN: 978-0-470-77269-0.

SIMCORE 2009. PAX2SIM Software. SIMCORE Corp. Available via <http://www.simcore.fr/Pages/en/en_index.php> [accessed August 26, 2009].

Spriggs, J. 2008. Airport risk assessment: Examples, models and mitigations. Roke Manor Research Ltd. Available via <http://www.roke.co.uk/download/papers/Airport_Risk_Assessment.pdf> [accessed August 26, 2009].

SPT 2006. SPT: Ideal process flow V 2.0. Available via <http://www.iata.org/NR/rdonlyres/31BD66A2-4446-4514-A911-3EA9DDAC7CAA/0/IPF_V20_FINAL.pdf> [accessed August 26, 2009].

Weiss, W. E. 2008. Dynamic security: An agent-based model for airport defense. In *Proceedings of the 2008 Winter Simulation Conference*, eds. S. J. Mason, R. R. Hill, L. Mönch, O. Rose, T. Jefferson, J. W. Fowler, 1320-1325. Available via <http://www.informs-sim.org/wsc08papers/158.pdf> [accessed August 26, 2009].

Wilson, D., E. K. Rose, and A. A. So. 2006. Security checkpoint optimizer (SCO): An application for simulating the operations of airport security checkpoints. In *Proceedings of the 2006 Winter Simulation Conference*, eds. L. F. Perrone, F. P. Wieland, J. Liu, B. G. Lawson, D. M. Nicol, and R. M. Fujimoto, 529-535. Available via <http://www.informs-sim.org/wsc06papers/065.pdf> [accessed August 26, 2009].

Xie, Y., J. Shortle, and G. Donohue. 2004. Airport terminal-approach safety and capacity analysis using an agent-based model. In *Proceedings of the 2004 Winter Simulation Conference*, ed. R .G. Ingalls, M. D. Rossetti, J. S. Smith, and B. A. Peters. 1349-1357, Available via <http://www.informs-sim.org/wsc04papers/177.pdf> [accessed August 26, 2009].

AUTHOR BIOGRAPHY

PRAVIR K. CHAWDHRY is a Principal Research Scientist at the Joint Research Centre of the European Commission where, as an Action Leader, he leads a research group in the Institute for the Security and Protection of the Citizen. He received his Ph.D. in Control Systems Engineering from the Queen's University of Belfast in 1985. He has worked as research scientist and Lecturer in engineering and design from 1986-2001 in the UK. His current interests are in the security of information and communications systems, identity management and biometrics in border control. He is member of the IEEE. His email is <Pravir.Chawdhry@jrc.ec.europa.eu>.