Curbing the congestion conundrum

With continuous growth still expected in worldwide air passenger traffic, a look at some of the solutions designed to maintain and increase security levels in airports

by Jean Salomon, IER

Airport security is a convoluted problem that requires the concerted use of various types of technologies and resources to carry out layered and interdependent preventive or curative tasks ranging from surveillance, tracing, tracking and monitoring, to detecting, deterring, blocking and defusing. Not only does this form of security have to deal with people on the move (passengers, crew, ground staff) and goods either in transit or stored on the premises, it must also take into account the aircrafts themselves, capable of becoming major security threats if in the hands of terrorists.

Via enabling processes and technologies such as biometric Fast Tracks, self-service kiosks, passenger triggered baggage drops and remote airport services, airport business processes are being re-engineered not only to match stringent environmental and budgetary constraints but to accommodate larger aircraft, growing low-cost carrier operations, and differentiated types of border crossing. To the eye of the observer, airports may appear to be developing in 3 dimensions, along one or more of the following lines:

- space (airport boundaries are being extended to our homes via Internet check-in);
- time (Advanced Passenger Information for border crossing or destination country immigration pre-clearance can be filed prior to airport check-in, by travel agents or at home, enabling passengers to qualify for "really fast" Fast Tracks);
- service functionality (origin-to-destination baggage pick-up and delivery would improve passenger flow in cluttered check-in areas).

All this aims at developing more seamless operations, able to absorb an expected 5% yearly increase in passenger traffic worldwide. Yet how can we pledge to maintain, or even increase, the current level of airport security?

The role of automation

Part of the answer to this pledge resides in increased or improved automation, whether for passenger travel document inspection (e.g. controlled/secured self-boarding), or for simultaneous passenger and carry-on luggage screening (e.g. deployment of millimeter wave technology to detect concealed non-metallic weapons or the spectroscopy breakthroughs needed to pick up liquid explosive components).

Contrary to what is usually claimed, this may not always lead to a reduction in processing times. However, automation does have two distinct advantages. Firstly, it will ensure that agreed security procedures are always performed and maintained, even when overworked agents are facing high numbers of passengers. Secondly, it will enable management to redeploy these agents to where they are most needed in the airport (a typical problem for understaffed immigration and customs offices).

In both cases, additional automation will favor an increase in security and efficiency, as well as improving passenger perception of the overall service provided by all stakeholders.

Secure self-boarding

One example that illustrates the benefits of automation is the Lufthansa "Quick Boarding Gate" deployed at Munich T2 airport. The QBG enables secure self-boarding, with flap-equipped access control portals used in parallel with manual boarding to automate inspection while avoiding tailgating (i.e. preventing two passengers from entering the same portal together to thwart inspection). Remote visual supervision by one single agent over several positions also contributes to the process economics and ROI. Extensive modeling and testing by the carrier and the manufacturer (IER) allowed for the balancing of seemingly conflicting parameters, such as that of accessibility with the prevention of fraudulent use, with many different passenger configurations, including children and various carry-on bags. Passenger acceptance has been very high, a decisive factor in ensuring smoother and faster access to the planes.

Automated border crossing

Another example is the use of an airport-driven Fast Track service, such as that in place at Amsterdam Schiphol airport. Paying "Privium" program members are firstly enrolled, their background checked and their iris biometrics captured and stored on a service smart card. They are then able to take advantage of a separate immigration fast lane using automated inspection via a live comparison of their iris biometrics with the card template. A turnstile-equipped obstacle with a side door either grants them direct border crossing in the case of a biometric match, or opens the side door, reverting them to document inspection by an immigration officer. Here again, local manpower optimization is possible. A single officer can perform his duties on all "standard" passengers (manual lane) while overseeing an automated gate, dealing with the Fast Track members who failed automatic clearing.

IER's "Quick Boarding Gate" at Lufthansa'a T2 Munich terminal

As ePassports and eID cards become more prevalent in the future, these types of border crossing processes are likely to develop even further, either as private paying initiatives, or as part of embedded free airport and immigration services. A similar paying experiment is being offered to frequent travelers at Orlando airport as an iris-enabled Fast Track to TSA security with no border crossing involved.

Limits to automation

There are, however, drawbacks and limits to automation. Three types of limits preclude the use of existing technologies or limit their development in our field of

The Privium Fast Track service at Amsterdam Schiphol airport (above); as well as improved passenger screening, automation will also enable luggage to be screened more effectively (below)

interest: legal aspects; performance vs. price constraints; and the core problem of identity management.

Firstly, in some countries, such as France, it is legally forbidden to use even the lowest radiation dose to perform a live x-ray on a passenger at a security checkpoint, even as a voluntary alternative to a pat-down. This very same screening procedure has recently been trialed at Heathrow on volunteers to by-pass pat-down agent search. Similar techniques are routinely performed in gold mines (South Africa), to monitor prisons, or to x-ray suspected drug smugglers.

Secondly, the cost vs. performance ratio could slow down the move towards higher levels of airport security, as is currently the case with EDS tomography scanners used to check passenger luggage for explosives. In view of the reduced explosive quantities that must be detected flawlessly by these instruments to meet updated TSA specifications, a fairly large ratio of useless "false alerts" ("False Positives") is necessary to keep the "misses" ("False Negatives", i.e. the catastrophic failure to detect a real threat) close to zero. This necessitates even higher EDS screening levels – going as far as baggage opening by a specialist - thus reducing the overall system throughput. Known technology add-ons to the existing EDS screening chain, such as diffracted x-rays, would keep the "False Negatives" close to zero while significantly decreasing the ratio of "False Positives", but would have a significant cost impact. Of course, there is room for improvement in detection processes, and such process is an ongoing one.

Thirdly, technology itself could become a threat to security. What would be the benefit of introducing hard-to-forge and more secure eMRTDs (Machine Readable Travel Documents), if the primary identity breeder document could be counterfeited relatively easily? Why bother with additional encrypted access to the chip data of the new ePassports (like the future EU mandatory EAC, Extended Access Control, to further encrypt the 2008 chip's fingerprint data) if the bearer can easily carry out identity theft at enrollment during ID verification of the breeder document? In the US, for example, where less than 21% of all citizens hold a passport, the initial verification of the official birth certificate of a passport applicant could become an operational quagmire. Security, as with all layered processes, is only as strong as the weakest link in the chain. Here, technological progress would grant the bearer of an assumed identity a cheap way to obtain a perfectly legitimate, high-tech and strongly protected "authentic" official ID document! Meeting such identity management challenges has become a central security problem which governments are currently addressing. It will gradually be resolved.

Automation as an equalizer, not a tranquilizer

Technology tends to be detrimental to security if applied on the wrong premises. An initial mistake in identity management could lead to undetected ID theft. Similarly, in the case of face biometrics, bypassing stringent quality controls over the ePassport bearer's digital picture initially collected at enrolment would reduce the reliability of later 1:n biometric searches in a watch list.

Automation and technology should therefore not be used for comfort, by analogy, or without control over process scalability and performance, as in this way they would merely serve as inappropiate "security tranquilizers". What matters is not which technology you select to automate reconciliation of the passenger name on his boarding document with the official ID presented, but that this reconciliation, if deemed mandatory, is automated in a flexible way and performed with

a proven and sustained level of efficiency. Automation and technology should therefore work as "security equalizers".

On the brighter side, in airports needing to realign business processes along the 3-D constraints described in the introduction, technology could play a major role as a key enabler.

A framework for progress

IATA's Simplifying Passenger Travel Interest Group (SPTIG) has developed an Ideal Process Flow diagram (IPF). The aim of this group of transportation industry organizations including airlines, airports, government control authorities and technology suppliers, is to try and identify bottlenecks, potential process duplication and to resolve conflicts of interest amongst the various stakeholders to provide air travelers a safer, seamless, faster, and more pleasant traveling experience.

SPTIG's IPF recommendations include the gradual blending of the traditional multi-step travel chain (reservation, check-in, security and boarding) into fewer processes, still intertwined, ideally leading to one single step-single stop model, centered around the security checkpoint. The SPTIG has so far identified three key success factors that match the 3-D airport environment described in the introduction:

• space. The ubiquitous use of an eToken (most probably an ePassport in the future) to access, or egress from existing airport secure/controlled areas;
• time. The networked sharing and real-time update of each passenger's security status, including watch list and blacklisted police database updates, at each point of interaction using the eToken. A quick security enhancement would be to automatically notify at the security checkpoint about a passenger "selectee" status, to raise the screening agent guard;
• functionality. The use of biometrics to carry out strong authentication only when needed, either during border control (coupled with security), or, if mandated by law, to prevent identity swaps during the boarding process.

The road less traveled

Yet another factor contributing to increased airport security lies in the anticipated growth of eMTRDs, and the development of large scale, IT-driven programs like the US-VISIT or the Schengen Information System, with their associated remote data collection programs, including biometrics for visas. Here, technology could almost be used as an alibi: the fact is that more than 20% of all visa applicants to the Schengen area are being denied access. Yet, all biometrics pre-collected during the application process (10 fingerprints) are being kept and remain accessible to Government Security Agencies, which could cross-fertilize national blacklists, subject to EU data privacy restrictions.

Today, while security technologies progress by attracting sizable investments, encouraging signs are visible:

• weak airport security links are being upgraded by introducing regular background checks of ground staff;
• biometrics-enabled access control to sensitive airport areas is superseding standard employees plastic badges;
• the traveler's learning curve has been fairly satisfactory for airport kiosks, partly based on their earlier experience with bank ATMs. Similarly, the observed increase of contactless card usage in mass transportation could help promote the success of the contactless, security-prone ePassports in airports, as a "can opener" to new services.

The cooperation of all stakeholders in the transport industry is key to easing up congestion at airports

However, the real key to global success lies in the cooperation of all stakeholders in the transportation industry to ease up congestion at major airports, while the latter strive for the ever safer and more secure handling of their passengers.