Plane sailing in the future?

An insight into some of the key issues for consideration if airports are to truly offer their passengers streamlined and secure travel from reservation through to boarding

by Jean Salomon, IER

According to Airports Council International (ACI) data, 2.2 billion air passengers emplaned last year, over 500 million of which at the world's 19 busiest airports. In the last 6 years, the number of non-US airports in the top 19 has increased from 6 to 9. In its forecast, ACI estimates a global doubling of passengers over the next 20 years, with Far East routes also growing at double pace, paralleling the respective growth ratio of the Far East GNP. By way of an example, Beijing airport has risen to 9th busiest airport in the world over the 4 last years. Such growing congestion (the number of worldwide air passengers has risen 4.8% since 2005) is resulting in a global quagmire that threatens to turn major airports into mass choke points.

In a recent study, Robert Poole of the Reason Foundation challenged the US TSA to restrict its activities to policy-making and regulation in an approach similar to that employed in major European airports. The challenge is to develop a renewed analysis based on risk assessment of the various congestion components linking the three major fluxes - documents, goods and people - with greater focus on TSA-approved security contractors operating under a TSA-designed (or TSA-approved) multi-modal, multi-layered airport security approach.

The focus of this article will be a small subset of the much needed business process realignment, which has been actively investigated by the IATA Simplified Passenger Travel Interest Group (SPTIG),

a multiple stakeholder group whose sole interest lies in promoting seamless, yet secure passenger travel. The focus is on streamlining the interaction between the passenger and the infrastructure during the 4 key steps of his journey: pre-travel (reservation), check-in, security checkpoints, and boarding.

The travel process: areas for improvement

There are several types of security improvement achievable in the present travel process breakdown:

Multiple authentication

Multiple authentication is required - unduly most of the time - at each of the four aforementioned travel steps. Could we reduce the number of these steps, if proved redundant, valueless, or – worse still - detrimental in terms of security? The answer is yes, providing we can correctly and dynamically correlate the flow of passengers and luggage through the premises with the appropriate counter flow of sensitive online information. This should integrate up-to-the-minute changes to the original passenger security status, his rough geo-location around the airport premises, and any associated last minute off-premises security updates (e.g. presence on a watch list or no-fly list) and on-premises behavior (e.g. active online CCTV tracking of suspicious passenger behavior, or an active "hit" during a security interrogation along an updated CAPPS procedure).

Process redesign, systems integration and - above all - stakeholder cooperation should be essential in refreshing the security status online and enabling each airport stakeholder to access the same up-to-date shared information on a given passenger, his luggage and his carry-on's.

Dynamically analyzing, retrieving and linking up-to-date passenger, goods (luggage) and information flows is the main backbone of a proactive security process, and allows the focus to be placed on the real threat: people, not products. Weapons and explosives do not crawl by themselves, they are carried by people!

Inefficient passenger authentication

Can the traveler prove to the security agent (or the automated device or system) in charge that he is the rightful holder of both an authenticated travel document and a specific flight reservation, be it boarding pass, electronic reservation or approved flight entitlement? Can the security process actively link a verified passenger's ID to his transaction request for the right to board? Are we really sure of the identity of every passenger boarding a flight? If ID verification is not performed at boarding, the answer is no.

This is typically the case in the US, where major airline-operated hubs mix domestic and international traffic. In such locations, all passengers that clear a single security checkpoint proceed en masse to multiple boarding gates downstream where, in the absence of any mandatory ID control, the carrier has no way of preventing ID substitution. This has a negative security impact: it could mean either losing track of a passenger discretely followed by Security, or allowing someone to become an undetected illegal alien (by swapping domestic and foreign destinations with an accomplice). Worse still, in the case of a disaster, the carrier would be incapable of providing a trusted list of victim IDs following a crash.

Yet, two equally simple remedies are available:

• either mandate a thorough ID check at each boarding gate (supposedly the last step before reaching one's seat). Here, visual reconciliation between the travel document (typically a passport or national ID card), the boarding document, and the passenger's face is performed by an agent. Tomorrow, self-boarding automation could prevail, with a biometric-embedded ePassport scrutinized, via facial or fingerprint capture plus 1:1 ID verification, coupled with an intelligent access portal able

IER's new generation of secure boarding, used by Air France for the CDG-AMS shuttle self-boarding trial at CDG 2F

to prevent tailgating

• or have a single security-checkpoint per departing gate area, where everything is performed (such as at Changi Airport, Singapore).

There are large inconsistencies between countries on this matter, which need resolving. As an example, contrary to the US, France empowers its national carriers by law and mandates them to always perform ID reconciliation and matching upon boarding.

One related ongoing trial is the new generation of self-boarding gates enabling the use of barcoded boarding passes (see image above). By coupling arrays of infra-red sensors with software control and studying sliced consecutive profiles of people and goods crossing the IR beam mesh, correct operational discrimination between passengers can be achieved, avoiding tailgating, yet letting hand luggage pass and maintaining acceptable passenger throughput across the gate.

A provision has been taken in this new generation to accommodate biometrics capture at the gate in the future to further automate passenger ID reconciliation with his PNR/API data through the DCS, thus meeting any future mandated ID-substitution avoidance challenge.

The growing congestion of airports has rendered essential the streamlining of the four major process steps that comprise passengers' journeys: reservation, check-in, security checkpoints, and boarding

Preventing non-travelers passing through security

There is presently no way to prevent non-travelers from entering the sterile area through a security checkpoint. This subject received great publicity when two journalists using a single A4 home-printed boarding pass and its photocopy successfully cleared a Manchester airport checkpoint. This problem has also been covered in official reports such as a 2006 report by the Records Management Association of Australasia: "A fake boarding pass would be nearly impossible for airport screeners to detect, because they have no access to airline databases at the screening checkpoint ".

An easy solution could be provided to prevent inadvertent or willful trespassing: equip the entrance of each checkpoint lane with a simple gate reader linked to the DCS' passenger list, and await the host response with respect to travelers' eligibility to undergo checkpoint examination. If a "not on any active flight list" message is returned from all local DCS's, passenger will simply be denied access and referred to secondary search. If an "already went through checkpoint" message is returned, the first likely reason is that the same passenger forgot something in the public area, backtracked to fetch it and came back again at the checkpoint. Stamping or tagging the boarding document (even manually) helps resolve the case. If, however, a "dupe" has also been found in the "boarded" passenger list, this points at a likely impostor. Here again, a bit of process improvement at the checkpoint could increase security at a fairly low cost, using already available equipment and IT infrastructure, simply by adding a query to the properly linked passenger list.

Improving border crossing procedures

What do ePassports really contribute to the further strengthening of security, particularly at border control? Hasn't technology unexpectedly turned into a showstopper? What about revising security policies? The answer to the first question is rather negative: although over 45 nations currently only deliver ePassports to their citizens traveling abroad, practical use of such documents is still fairly low, because most of these same countries have not yet installed the required ePassport RFID reader infrastructure at their own border control airport checkpoints. Thus, despite strong progress in ePassport interoperability, no large-scale benefit has been reaped from more secure e-travel documents as yet.

Secondly, it looks as if, for the time being, alternative technologies will be used rather than the globally interoperable ones decided upon: as long as there is no e-reader infrastructure in place in major airports, no biometric authen-

tication can be performed on the travel document bearer - not even on the ePassport of a traveler returning to (or leaving) his own country.

Thus, mass deployment of globally interoperable processes such as Automated Border Clearance (ABC) or ID reconciliation at secure self-boarding portals using ePassports (or contactless eIDs) as common eTokens will be put back even further, perhaps another year. Large-scale programs that have been successful up to now have essentially been customized for registered travelers, and operate by using biometrics not yet implemented by ICAO, mostly with proprietary travel entitlements (cards) securely delivered following background checks at the enrolment stage. These programs have become marketing tools that benefit the airports (e.g. the "Privium" border crossing paying program in Amsterdam). Only now are we seeing the final testing of a global face biometrics deployment using ePassports for all citizens of a country (i.e. the 2nd generation of the "Fast Gate" automatic immigration process for all Australians holding an ePassport).

Thirdly, Customs and Immigration resources should be redeployed to where they are most needed to focus on potentially greater threats relating to certain individuals and goods. Ultimately, tracking and tracing progress cannot be achieved if there is no link between in-bound and out-bound security passenger procedures. This might significantly change national security laws and policies, such as the last UK move to implement out-bound border control for all its nationals leaving through a UK airport.

Robust and correlated document, goods and people flows are the pillars of a resilient airport security pyramid

Taking a proactive approach

Airports have to live with interim security measures which are necessary, for example, to contain threats resulting from insufficient technology breakthroughs: metal detectors will ultimately be superseded by both millimeter wave imaging and scatter x-ray combined with spectroscopic remote goods analysis, to detect non-metallic weapons and dynamically assess hidden threats from liquids or solids carried by a passenger (on his body, in his clothing or carry-on).

Also, better preparation of required security process updates is required before launching future portal deployment, to avoid the costly and overreactive measures after 9/11. Yet, in terms of security, airports must continue to progress by adopting a proactive attitude:

- Impose biometrics entrance/exit control to all staff at all airport security checkpoints, including geo-location and history
- Develop a biometrics-enriched cross-linking infrastructure between all available secure information flows
- Actively cooperate with other industry stakeholders, so that the elimination of a local choke point, even if carried out with improved security, does not result in the creation of yet another queue somewhere else down the path.

Robust and highly correlated document, goods and people flows are the three basic pillars of a resilient global airport security pyramid. "Elevators" to the security pyramid will essentially rely on interoperable e-authentication tokens using biometrics.

Linked automation tools such as "sniffers" and portal access control will be key to further bolstering airport security, both for border crossing and secure boarding, only if continuous, dynamic threat adjustment procedures are conducted in a concerted way across all stakeholders' networks.

The ease with which non-travelers have been able to pass through security with fake boarding passes has outlined the need to equip checkpoint lanes with readers that can cross-check against departure control system passenger lists