Watching through the “I”s of aviation security

Sheldon H. Jacobson

Received: 14 June 2011 / Accepted: 16 June 2011 / Published online: 23 June 2011
© Springer Science+Business Media, LLC 2011

It has been ten years since September 11 (9/11). In no other facet of society have the events of that day had a more enduring effect than on aviation security operations. With the creation of the Transportation Security Administration (TSA) came technologies like explosive detection systems (and 100% checked baggage screening), trace devices, puffers, and advanced imaging technologies (more commonly known as full-body scanners), and policies requiring passengers to remove their shoes and carry liquids and gels in 3-1-1 bags, all designed to secure the air system. With all these changes, are we really safer after the tens of billions of dollars spent? Has the TSA provided a cogent argument that their strategy yields a more secure system for air travellers as we move into the second decade after 9/11?

Based on the approach taken by the TSA, as evidenced by aviation security operations at airports, and research conducted on the use of aviation security technologies and procedures, I posit that as we look into the future and evaluate the trajectory of aviation security, based on the decisions of the past decade, the air system is at the riskiest point that it has been since 9/11.

Jacobson and Lee (2010) describe how aviation security can be broken down into the three “I”s of screening: Items (threats), Identity (passengers), and Intent (people). They note that stopping threat items and matching passenger identity are surrogates for measuring malicious intent. The rationale for this deduction is that passengers who attempt to carry threat items (like firearms, knives, or explosives) onto an airplane are also likely candidates for inflicting harm to the air system. The same can be said for passengers who attempt to hide or misrepresent their identity. The key point is that screening for threat items (or validating identity) is neither necessary nor sufficient for thwarting future terrorist attacks.

S. H. Jacobson (✉)

Simulation and Optimization Laboratory, University of Illinois, Urbana, IL 61801, USA
e-mail: shj@illinois.edu
URL: netfiles.uiuc.edu/shj/www/shj.html

Since 9/11, each change in aviation security operations as been instituted after, not before, attempted threats attacks. The 2001 “shoe bomber” incident led to the shoe removal and screening policy, while the 3-1-1 liquid and gel bag policy was instituted after the 2006 plot to blow up planes bound for the United States with liquid explosives. More recently, the 2009 Christmas Day bomber incident, where the passenger was carrying explosives in their undergarments, led to the deployment of advanced imaging technologies and pat-downs for all passengers. In all these cases, the policy changes followed the terrorist incident. Were we unaware of such threats apriori? Are there other threats lurking on the horizon that the aviation security system is ill-prepared to defend against? Even before each of these security operation changes, the intended threat attack was thwarted with existing technologies and procedures. If the TSA continues to chase the next threat items, are they not effectively looking in the rear view mirror while terrorist threats move forward? The TSA can make important strides to improve airport security by paying attention to the real threats, which are individuals with intent to cause harm.

Advanced imaging technologies provide their own unique set of challenges, given how they are utilized to identify threat items and the false sense of security that they provide. Current throughput rates for such devices are inadequate to handle all passengers at airport checkpoints in real-time, particularly at high volume airports during peak travel periods, and hence, are ill-equipped to be used for primary screening. This means that not all passengers can be screened using such technologies. The strategy in place to screen passengers for threat items is tantamount to flipping a coin, based on whether the advanced imaging technology device is available when a passenger reaches the checkpoint screening location. An arbitrary random decision-making process is certain to be less effective than even the most rudimentary prescreening rules (based on passenger behavioral information and CAPPS, the Computer-Assisted Passenger Prescreening System, and its various incarnations and enhancements) applied to funnel people to or away from advanced imaging technologies. If Albert Einstein believed that God did not play dice with the universe, then travellers should expect that the TSA not play dice with their lives. Moreover, any security strategy based on the premise that all passengers provide the same security risk and hence, require the same level of security screening is fundamentally flawed and inherently dangerous when the security operations in place cannot support such a strategy. Such a situation induces intelligent threat attackers to game the system by timing their arrival to security checkpoints and overwhelming the system using decoy passenger to divert and cloud security attention away from themselves. Research on this very issue is described in the literature (e.g., McLay et al. 2009, 2010, Lee and Jacobson 2011). Threat attackers can also enter the air system through regional airports, where it would not be cost-effective to deploy advanced imaging technologies, resulting in a gaping security hole. All these points illuminate the vulnerability of the air system and the risk of deploying and utilizing advanced imaging technologies in the current manner.

With ballooning federal budget deficits, there will be limited resources available to protect the air system well into the foreseeable future. Thus, the inappropriate use

of resources for screening passengers (and their baggage) for whom there is effectively zero risk (such as passengers for which significant information is voluntarily provided and available) means that the same resources are unavailable to screen passengers (and their baggage) for whom less information is available and greater security scrutiny is justifiable. One can claim that in the name of fairness, all passengers must be treated the same. However, it is truly fair to arbitrarily use, and waste, scarce security resources and subject zero-risk passengers to unnecessary threat item screening?

So what needs to be done? First, the one-size-fits all approach to passenger and baggage screening must be replaced with a system that directs technologies and procedures more judiciously (Jackson et al. 2011). To move in this direction, focusing more on identity, instead of attempting to identify potentially malicious individuals, use data gathering capabilities and sources to identify who they are not. Terrorists covet anonymity and secrecy. CAPPS provides data analysis that may lead to 60%-70% of passengers being safely exempt from advanced imaging technology screening and enhanced pat-downs, and their accompanying baggage exempt from screening with explosive detection systems. The cost savings of such a strategic shift would be enormous, without sacrificing security. Second, when passengers are legitimately flagged for enhanced screening, create a data base to collect such information so that it is not lost, since terrorists are testing airport security systems to identify vulnerabilities (and be certain, they will find them). The resulting data will reveal patterns that provide clues to better enhance intelligence gathering and data mining. Without such memory, existing security will remain mired in the never ending search for threat items, without the ability to move forward in capturing terrorist identities and egregious intent.

To justify expenditures on new technologies and procedures, the TSA claims that advanced imaging technologies and enhanced pat-downs are necessary, for now. They also state that this is as far as threat item screening will be taken. What changes will the TSA implement after a suicide bomber brings down an airplane using an explosive device (possibly lodged in a body cavity) that circumvents such technologies? Where will this mindless threat item screening tactic end?

The events of 9/11 were not a failure in aviation security operations. They were a result of flawed aviation security policies in place at that time. The phrase “risk-based security” is being mentioned and discussed within the TSA, though it is not clear exactly what this means and how it would change current security operations. The TSA strategy of using layers of security systems is indeed the right approach. The key to improving security well into the future is to define, implement, change, and continually update the available layers of security appropriately. The current react and spend approach to security will lead those with intent to attack the air system to identify gaping holes and pass through them unscathed, resulting in an event that the TSA operations were designed to prevent. Employing subtle changes in today’s security strategies (e.g., target screening that refocuses when advanced security technologies and intrusive screening procedures are used) can make the entire air system more secure and convenient for the majority of travelers, and more onerous and challenging for those intent on causing harm to the air system. Keep an “I” out for it.

Acknowledgements Sheldon H. Jacobson has been studying aviation security operations since 1996. His current research is supported in part by the Air Force Office of Scientific Research (FA9550-10-1-0387) and the National Science Foundation (CMMI-0900226). The views expressed in this paper are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, National Science Foundation, or the United States Government.

References

- Jacobson SH, Lee AJ (2010) Aviation security in 2030: A glimpse into the future. *ORMS Today* 37 (6):14–16
- Jackson BA, Chan EW, Latourrette T (2011) Assessing the Security Benefits of a Trusted Traveler program in the Presence of Attempted Attacker Exploitation and Compromise. Working Paper, Rand National Security Research Division, Santa Monica, CA
- Lee AJ, Jacobson SH (2011) The impact of aviation checkpoint queues on optimizing security screening effectiveness. *Reliab Eng Syst Saf* 96(8):900–911
- McLay LA, Jacobson SH, Nikolaev AG (2009) A sequential stochastic passenger screening problem for aviation security. *IIE Trans* 41:575–591
- McLay LA, Lee AJ, Jacobson SH (2010) Risk-based policies for airport security checkpoint screening. *Transp Sci* 44(3):333–349