

# Airport Safety: A Case Study for Infrastructure Security<sup>i</sup>

*The current implementation of do-not-fly lists and the use of documents to authenticate passenger identity won't necessarily improve airport security.*

**By M. E. Kabay, PhD, CISSP<sup>ii</sup>**

An opinion piece in a recent issue of *US News & World Report*<sup>iii</sup> defending the internment of Japanese Americans during the Second World War has pushed me over my limit in tolerating fuzzy thinking about infrastructure security, so in this article I'm going to use airport security as a focus for what I hope you will find to be a bit of clear thinking.

I will dissect what I see as serious errors of reasoning that are harming our ability to ensure passenger safety in this country. On the way, I'll also take some swipes at other aspects of public policy on infrastructure security.

My hope is that readers will be sufficiently (a) convinced and (b) incensed by the foolish waste of our defense resources to speak out in their professional capacity and influence public policy for the better. *ACM Ubiquity* readers have the professional background and the intelligence to be able to intervene in these matters -- get on with it!

## **1 Names**

As most readers know, *authorizing* access to resources involves both *identification* and *authentication* (I&A). However, the key question for security is whether the person asking for authorization is *trustworthy* for the specific functions in question. For example, at an airport, we want to know whether we should trust someone on a plane as a passenger. Now, when we consider candidates for a job, we investigate their background. The thoroughness of such investigations depends on how much harm the candidates can do if they are Bad People. At an airport in the USA, there is usually no background check.

Knowing someone's *name* means nothing in itself. For example, if Timothy McVeigh had walked up to an airline counter on April 18, 1995 (the day before the bombing of the Murrah Federal Building) and used official documents showing that he called himself "Timothy McVeigh" I doubt that an airline clerk would

have stopped him from boarding a plane. At that time, nobody at the airport would have known anything about him.

Thinking that knowing someone's name -- and nothing else -- has given one sufficient information to judge that the person is or is not a threat is an elementary error of reasoning. It is an example of what anthropologists and psychologists call "magical thinking:" believing that knowing a being's name gives one power.

But alas, finding out what a person claims to be called does not in itself tell us that the person is good or bad and it does not in itself improve airport security.

## 2 Papers

In the first part of this paper, I suggested that knowing what people call themselves is not in itself a sound basis for trusting them.

Ah, but airport personnel are much too savvy simply to ask people what they call themselves, right? Airline clerks also ask for *proof* of that identification, so that must make things safer, right?

Well, no.

As readers know, deciding whether to authorize access usually requires both identification and authentication (I&A). Identification consists of presenting an identifier (duh): a name or label. Authentication is the *binding* of an identifier (e.g., "John Smith") to a specific entity (the John Smith born in Toledo on May 13, 1943, whose Social Security Number is 123-45-6789; who married Jane Morrison on June 12, 1965; who is the father of twin daughters named Julie and Sandy born on December 27, 1969; who lives at 234 Road Street in Townsville, Ohio; and who works at Acme Corporation in the Accounting Department; whose Scottish Terrier pup is 18 months old and called Josh – *that particular* John Smith).

But the airport clerk doesn't know or care anything about that particular John Smith; the rules say that as long as the John Smith in front of him or her has a piece of paper that also says "John Smith" then it's OK to let him on the plane.

As readers will recall, there are four ways to authenticate the user of an identifier: what they know (that others don't), what they have (that others don't), what they are (that others aren't), and what they do

(that others do differently). These phrases refer respectively to passwords or pass phrases, tokens such as keys or cards or passports, passive biometrics such as fingerprints or iris patterns and dynamic biometrics such as voice prints or keystroke dynamics.

We say that an authentication method is "strong" when the authenticator makes it difficult to impersonate the authorized user of the identifier. At an airport, for example, no one is going to propose using a red poker chip as the basis for authenticating the identity of John Smith to decide whether the person calling himself that should get on a plane; it's too easy to get red poker chips. Token-based authentication makes sense only if the token is relatively difficult for a Bad Person to obtain or to fabricate.

But at airports I've gone through, people are being asked to identify themselves using commonly available tokens: documents such as drivers' licenses. You can get a driver's license in Vermont by showing a clerk a bill from a utility; if it includes the name you are using in your application, the address you are using in your application, and the name on some other form of identification, you can have a driver's license on the spot, complete with color photo and lamination.

We establish a *chain* of trust from the *certifying* authority (here, the Department of Motor Vehicles -- DMV -- in Vermont) to the next authority granting privileges (here, the airline clerk at the airport who issues a boarding pass based on the driver's license) and on to the final user (in our example, perhaps the ticket-taker letting passengers onto the plane based on the boarding pass).

But how strong is the original authentication for your name that is provided by a utility bill shown to the DMV clerk? And therefore how strong is the chain of trust conferred on your name by a driver's license granted to anyone who can produce a paper that looks like a utility bill and claims to be the person referenced on that sheet of paper?

You will recall that forgeable tokens are not a sound basis for authentication.

With minimal cost and effort, anyone can scan a utility bill and alter it to make it look as if it belongs to, say, Santa Claus who resides at 1234 State Street, Montpelier, Vermont. So how does presenting a utility bill stop a terrorist from getting a driver's license -- that magic key to getting on board an airplane?

And have you looked at your own driver's license recently? I just scanned mine on a \$75 scanner and created a 600 dpi color image of it which I then proceeded to alter so that it shows images of one of my cats -- one in full intensity and a little one at half intensity -- right on top of my original images.

Does anyone think that there are terrorist organizations unable to create as many fake drivers' licenses as they need to get on planes?

So demanding papers of dubious strength to authenticate identity doesn't in itself materially improve airport security either.<sup>iv</sup>

### 3 Lists

In this section I discuss the Do-Not-Fly list (DNFL) maintained by the US Transportation Security Administration (TSA). The DNFL appears to consist of names with little or no additional identifying information.

There are now many articles appearing in national newspapers recounting horror stories of inoffensive travelers stopped from boarding planes in United States because their names have been listed on the DNFL.

If the TSA is really using names without any other identifying characteristics as the basis for stopping people from flying, you have to question their commitment to the rule of law and the power of common sense. I don't know how many people will be blocked if a single "John Smith" ever makes it onto that list. Senator Ted Kennedy was stopped from boarding three US Airways flights in March 2004 because the name "Edward Kennedy" was on the DNFL. He got on the planes after his aides called for help from Tom Ridge, Secretary of Homeland Security. How many Edward Kennedys won't be able to get through to the Secretary of Homeland Security when *they* are stopped?

Deirdre McNamer (how appropriate) wrote a story in *The New Yorker* magazine in October 2002 about a 28-year-old pinko-gray-skinned, blue-eyed, red-blond-haired criminal called Christian Michael Longo who used the alias "John Thomas Christopher." His alias was placed on the DNFL used by the TSA. He was arrested in January 2002 but his alias was not removed from the DNFL. On March 23, 2002, 70-year-old brown-skinned, dark-eyed, gray-haired grandmother Johnnie Thomas was informed that she was on the master terrorist list and would have special security measures applied every time she flew. Indeed, the poor lady found that she was repeatedly delayed by a scurry of activity when she presented her tickets at an airline counter, extra X-rays of her checked baggage, supplementary examination of her hand-baggage and extra wandering at the entrance gates. On one occasion she was told that she had graduated to the exalted status labeled, "Not allowed to fly." She discovered that there was no method available for having

"her" name removed from the DNFL; indeed, one person from her local FBI office dismissively told her to hire a lawyer (although ironically, he refused to identify himself). An employee of the TSA informed her that "four other law-abiding John Thomases had called to complain."

In summary,

- (a) The basis for being included in the DNFL is undocumented.
- (b) There is no mechanism for informing people that they have been included (other than being refused boarding at the airport).
- (c) There is no standard procedure for being removed from the list (unless you happen to know the Secretary of Homeland Security, I suppose).
- (d) In general, lists of names alone, devoid of clear binding to specific people, are not an effective basis for identifying threats to security.

One final question: Is the DNFL consistent with the ideals of the land of the free and the home of the brave?y

#### **4 Profiles**

I'd like now to demolish arguments in favor of racial and ethnic profiling as a security measure.

Imagine that the United States population included about 1 million people of Albigensian descent. Suppose a group of Albigensian terrorists cause terrible things in the USA and so, egged on by jingoistic talk-show hosts and narrow-minded politicians, some people in authority decide to harass and even imprison Albigensians as a way of demonstrating their commitment to protecting citizens of the USA. The government arrests 120,000 Albigensian-Americans, of whom 80,000 are native-born US citizens. The Albigensians are forced to abandon their homes and property at enormous economic loss and are kept behind barbed wire in violation of *habeas corpus*: that is, without charge, without access to information about why they are being interned (beyond being told they are a threat to national security), without access to attorneys, and without any definite date for release.

In *US News and World Report*, a columnist sneers at people objecting to the incarceration of the Albigenians as closed-minded orthodox thinkers and justifies the extra-judicial imprisonment by writing that "It is always reasonable to look in the direction from which the gravest danger is coming" and smirks that the attacks against the USA were not carried out by "militant Swedish nuns."

Well, in our scenario, we aren't attacked by American Albigenians, either.

So what's the problem with this kind of ethnic profiling? Why shouldn't we apply the same logic at airports that has made DWB (driving while black) an offense punishable by summary arrest, pepper spray in the eyes, and repeated humiliations? Shouldn't interrogating Albigenians be a useful security measure?

No, it isn't. We shouldn't apply ethnic profiling because (a) it doesn't work; and (b) it violates the fundamental principle of law that demands impartiality and fairness in the application of laws.

The problem with ethnic profiling is that the people who are using it do not understand that there are two parts to the simplest comparison of behaviors. Let's return to the Albigenians. All of the attackers in our little psychodrama were Albigenians. Therefore, the defective reasoning goes, it makes sense to investigate / interrogate / incarcerate all Albigenians in America to protect Americans. Yes, but there's much more to consider.

First of all, in our story, the attackers were not Albigenian-Americans, they were Albigenian terrorists from Albigenia. Second, even if they HAD been Albigenian Americans, the question is what proportion of Albigenian-Americans are terrorists compared with the proportion of non-Albigenian-Americans who are terrorists.

The numbers might work out to a few dozen? a few hundred? Albigenian-Americans posing a threat and roughly a million not posing a threat. The numbers for non-Albigenian Americans might be a few hundred? a few thousand? militant anti-government gun-toting militia members and several hundred million not posing a threat. If that difference in proportion is supposed to justify mass suspicion and punishments, then Scottish- and Irish-Americans should have been in serious trouble after Timothy McVeigh bombed the Murrah building in 1995. Or are Scottish- and Irish-Americans off-limits when considering mass suspicion and punishments?

The only way this kind of racial or ethnic profiling seems fair is when its defenders are not targets. It's easy for people with underdeveloped moral reasoning to dismiss violations of fundamental justice as long

as the injustice is seen to apply to "others" and not to "us." It's easy to excuse abuse by pointing to "times of war" and "great danger" but such excuses play into the hands of demagogues and dictators. German anti-Nazi pastor Martin Niemöller warned of the dangers of silence in the face of such ethical corruption in his famous confession: "First they came for the Jews. I was silent. I was not a Jew. Then they came for the Communists. I was silent. I was not a Communist. Then they came for the trade unionists. I was silent. I was not a trade unionist. Then they came for me. There was no one left to speak for me."

Pouring investigative efforts into mass screenings of entire populations where the rate of success is on the order of million-to-one odds is a complete waste of scarce resources. It's also a moral obscenity.<sup>vi</sup>

## **5 El Al**

I'd like to look at a model that has demonstrably worked.

El Al is the Israeli national airline. "The only successful hijacking of an El Al plane was in 1968 when a flight from Rome was hijacked by members of the militant Popular Front for the Liberation of Palestine and forced to land in Algiers."<sup>vii</sup>

The airline uses a number of measures during check-in that focus on the behavior of specific passengers rather than primarily on names, documents, and lists.

- At the time of booking, every passenger's name is cross-referenced against several lists of known and suspected terrorists, including information from "Interpol, the FBI, Shin Bet (Israel's intelligence service) and others."<sup>viii</sup>
- Airline personnel are trained in interrogation techniques; many have military experience (in Israel, most people serve in the Israel Defense Force). They ask specific, pointed questions about each passenger's travel plans, where they bought their ticket (the agents check codes on the tickets to verify the answers), whom they are visiting and their relation to the traveler, and where they have traveled in the world and why. They introduce unexpected questions to keep people off balance even if they have prepared for interrogation. Every page and every stamp in the passport is examined; travel to countries viewed as enemies of Israel sparks additional probing questions.

- The questioners watch the traveler carefully during this interrogation, looking for any sign of nervousness or unusual reactions. Plain-clothed security personnel circulate among the passengers and observe whether they are traveling alone or with companions. Travelers who chat with others are asked what they talked about and their relation to those other people. The plain-clothed observers continue to watch the traveler during the interrogation to provide another perspective on whether there is reason for even more thorough questioning.
- Interrogation may be repeated once or twice more before the passenger is allowed to board.
- All baggage is carefully examined. What is the history of the bag? Where in the world has it been used? Who used it last? All luggage is checked for residues of explosives passed through a depressurization chamber to detonate altitude-sensitive bombs. Baggage transferred from other airlines must go through full security screening before being loaded onto the El Al flight.
- Anyone who seems to justify further investigation is delayed until the agents are satisfied; such people may well miss their flight as a result. In any case, all passengers are required to arrive at least three hours before their departure time because of the delays caused through this high security approach to air travel.

Additional measures make flights safer. El Al guards its planes 24 hours a day, including while they are being cleaned and serviced, in any airport in the world. El Al flight schedules are often changed in an attempt to interfere with terrorists' plans. Several armed, undercover, fully-trained security agents fly every El Al flight in aisle seats. The pilots' reinforced bullet-resistant door is never opened during flight no matter what happens.

The most controversial measures used by El Al security involve profiling. El Al personnel classify passengers as "low-risk (Israeli or foreign Jews), medium-risk (non-Jewish foreigners) and extremely high-risk travelers (anyone with an Arabic name)." In addition, "Single women also are considered high-risk, for fear they might be used by Palestinian lovers to carry bombs." [5]

Personally, I don't see these ethnic and gender profiles being acceptable in the USA for domestic travel.<sup>ix</sup>

## **6 Costs**

Could we apply security measures similar to those of El Al in the USA? One of the major issues is cost. Given the parlous state of US airlines, it is unlikely that additional costs occasioned by new security measures could be absorbed by the companies and employees through lower profits and reduced salaries.

So how much more would a ticket cost when the costs of El Al-style security were added to tickets prices? Estimates of the annual cost of security for El Al are in the \$90M range for about 15,000 flights a year. That's at least \$6,000 per flight. In contrast, the US Bureau of Transportation Statistics (BTS) reports around 9M flights a year in the USA.<sup>x</sup> Thus security would funnel a good deal of money into the pockets of airline employees responsible for security.

But the question is how much extra such security would cost per passenger per flight. The BTS report cited above shows 638,902,993 passengers on 8,951,773 flights, or an average of about 70 passengers per flight in 2000, implying a shared cost of about \$85 per passenger per flight (\$6,000/70) for security. This estimate doesn't count the existing costs of security measures in place already in the USA, which might reduce the incremental cost per passenger per flight for raising security to the El Al level. It's surely worth investigating further.

\* \* \*

I hope you have found this case study interesting. Whether you agree with my conclusions is not the point: *thinking about the issues* is the point. However, it's just one example of where you can turn your analytical thinking. There are many other infrastructure protection issues to which you can and should contribute. For example, are we protecting our coastlines effectively? How is our political rhetoric about homeland defense measuring up to actual expenditures for training and equipment for local emergency response teams in our own communities? Are the power plants / water supplies / transportation hubs in your own communities adequately protected? What are the security implications for local communities of the departure of National Guard troops for extended service overseas?

Readers, I hope you will get involved in these issues and contribute your intelligence and initiative to improving national infrastructure protection. Please join your local chapter of the InfraGard to share your thoughts with colleagues.<sup>xi</sup>

Now go out there and think for yourselves.

Notes

i This paper originally appeared as a series of columns in my *Network World Fusion Security Newsletter*. Archives are at < <http://www.nwfusion.com/newsletters/sec/> >

ii Associate Professor of Information Assurance / Division of Business & Management / Norwich University, Northfield, Vermont  
<mailto:mkabay@norwich.edu> <http://www2.norwich.edu>

iii Leo, J. (2004). The internment taboo. US News & World Report (24 Sep 2004).  
< <http://www.townhall.com/columnists/johnleo/jl20040920.shtml> >

iv For Further Reading:

Destkop counterfeiting. < <http://www.sgrm.com/art20.htm> >

Gilmore, J. (2003). Gilmore v. Ashcroft – FAA ID Challenge FAQ. < <http://freetotravel.org/faq.html> >

Havlen, N. & A. Harvey (2004). Wife turns husband in for forging immigration papers. < <http://tinyurl.com/3lg82> >

Passport fraud. < <http://tinyurl.com/5kqeh> >

v For Further Reading:

ACLU sues over Feds' "do not fly" list. < <http://seclists.org/lists/politech/2004/Apr/0015.html> >

Gathright, A. (2002). No-fly blacklist snares political activists. < <http://tinyurl.com/4q5jc> >

McNamer, D. (2002). Here's Johnnie. < <http://www.newyorker.com/talk/content/?020513tatlkmcnamer> >

Miga, A. (2004). "Terrorist Teddy" can't catch flight. < <http://news.bostonherald.com/national/view.bg?articleid=40687> >

Myers, L. (2004). Report: 'No-fly' list still lacking. < <http://www.msnbc.msn.com/id/6083667/> >

vi For Further Reading:

A History of the Japanese-American Internment. < <http://www.fatherryan.org/hcompsci/> >

Cockburn, A. & J. St. Clair (1999). Driving While Black. < <http://www.counterpunch.org/drivingblack.html> >

Leo, J. (2004). The internment taboo. US News & World Report (24 Sep 2004). <

<http://www.townhall.com/columnists/johnleo/jl20040920.shtml> >

Niemöller, M. (1945). < <http://motlc.wiesenthal.com/text/x00/xm0076.html> >

vii BBC (2002). EI AI sets security standards. < <http://news.bbc.co.uk/2/hi/americas/2097352.stm> >

viii Walt, V. (2001). Unfriendly skies are no match for EI AI. < <http://www.usatoday.com/news/sept11/2001/10/01/elal-usat.htm> >

ix For Further Reading:

- CNN (2001). Model for air travel security may be EI AI.  
< <http://archives.cnn.com/2001/WORLD/meast/09/26/rec.el.al.security/> >

- CNN (2002). EI AI secure because it must be.  
< <http://archives.cnn.com/2002/WORLD/meast/07/04/el.al.security/> >

- Verton, D. (2003). Q&A: Former EI AI security chief Isaac Yeffet on border, airport security: He remains skeptical of the money being spent on IT for security.  
< <http://www.computerworld.com/securitytopics/security/story/0,10801,81428,00.html> >

- Walt, V. (2001). And you thought getting to Israel was tough?  
< <http://www.usatoday.com/news/sept11/2001/10/01/elal-usat.htm> >

x BTS (2000). Summary of aircraft departures and enplaned passengers... 2000. < <http://tinyurl.com/5xhsw> >

xi National InfraGard Home Page. < <http://www.infragard.net/> >

Source: *Ubiquity*, Volume 5, Issue 34, Oct. 27 - Nov. 2, 2004, <http://www.acm.org/ubiquity/>