Insecure Flight: Broken Boarding Passes and Ineffective Terrorist Watch Lists

Christopher Soghoian

Indiana University Bloomington, School of Informatics
Indiana, USA
csoghoian@gmail.com

Abstract. In this paper, we discuss a number of existing problems with the airport transportation security system in the United States. We discuss two separate, yet equally important issues: The ease with which a passenger can fly without any identification documents at all and the ease with which print-at-home boarding passes can be modified, tampered with, and faked. The significance of these vulnerabilities becomes clear when viewed in light of the US government's insistence on maintaining passenger watch lists, whose contents are secret and effectiveness depend upon the government being able to verify the identity of each flying passenger. We then introduce a method of determining if any particular name is on the no fly list, without ever having to step foot into an airport. We introduce a physical denial of service attack against the Transportation Security Administration (TSA) checkpoints at airports, distributed via an Internet virus. Finally, we propose technical solutions to the user modifiable boarding pass problem, which also neutralize the physical denial of service attack. The solutions have the added benefit of meshing with TSA's publicly stated wish to assume responsibility for verifying passengers names against the watch lists, as well as enabling them to collect and store real time data on passengers as they pass through checkpoints, something they are currently not able to do.

1 Introduction

Since September 11 2001, the US government has placed tens of thousands of American travelers on watch lists as part of a massive security initiative that affects all of the nearly seven hundred million passengers who fly within the United States annually [17]. The Transportation Security Administration (TSA) supplies airlines with two watch lists, against which their staff must compare each passenger who flies. The watch lists contain names of people barred from boarding a commercial aircraft unless they are cleared by law enforcement officers (the "no fly" list) and those who are given greater security attention (the "selectee" list) [52, 36]. Before September 11 2001, the government's list of suspected terrorists banned from air travel totaled just 16 names. There are now over 44,000 passengers on the no-fly list, while the selectee list contains at least 75,000 names. Some of the most dangerous terrorists are never listed on either of the watch lists, as the intelligence agencies that supply the names do not want them circulated to airport employees in foreign countries for fear that they could end up in the hands of the terrorists [24].

Please use the following format when citing this chapter:

Soghoian, C., 2008, in IFIP International Federation for Information Processing, Volume 261; *Policies and Research in Identity Management*; Eds. E. de Leeuw, Fischer-Hübner, S., Tseng, J., Borking, J.; (Boston: Springer), pp. 5–21.

The concept of a no-fly list is premised on the idea that the government knowing who someone is can make airports safer. This idea is not universally accepted, and there are many researchers and commentators who strongly disagree with it [19]. In fact, the very definition of a "suicide bomber" means that there cannot be repeat offenders. This issue is beyond the scope of our paper as, useful or not, the US government wishes to have a no-fly list. We focus instead on the accuracy and effectiveness of the watch lists, and in highlighting the ways in which one can currently evade them.

The government's no-fly list is far from accurate [2]. It currently contains the names of 14 of the 19 September 11 hijackers and Saddam Hussein, all of whom are dead. It lists the name of convicted terrorist Zacarias Moussaoui, who is serving a life sentence in Colorado, and Evo Morales, the current elected president of Bolivia. Every flying passenger named Robert Johnson, Gary Smith or John Williams is subjected to an automatic and vigorous secondary screening, because at some point, suspected terrorists used these names as aliases. Even U.S. Senator Edward Kennedy found himself unable to fly for some time, although he was later able to personally demand that TSA clear his name. One reason for the high frequency of false positives for common names is because passengers are matched against the no-fly list by name only, instead of a combination of identity components such as date of birth, birthplace, current address or photograph [24].

Over 30,000 passengers have asked TSA to clear their names after being mistakenly linked to names on terror watch lists [31]. In January 2007, TSA Assistant Secretary Kip Hawley appeared before the US Congress to announce that the size of the no-fly list would be halved as a new more accurate list was introduced. He also announced that TSA was introducing a Traveler Redress Inquiry Program that will act as a central processing location for all passenger complaints that involve the no-fly and mandatory selectee lists [20].

TSA has been advocating for a number of years to be given the responsibility of checking passengers' names against the government watch lists, a task that airlines currently perform. Secure Flight is one of several attempts by TSA to perform airline passenger prescreening in-house. This program is intended to compare passenger information from Passenger Name Records, which contain information given by passengers when they book their flights, against watch lists maintained by the federal government [35]. The program, in development for over 4 years and at a cost of 140 million dollars, was suspended and sent back to the design stages in February of 2006 after investigators from the Congressional Goverment Accountability Office found that "TSA may not have proper controls in place to protect sensitive information" [4]. Assistant Secretary Hawley recently announced that the program is not expected to be complete until 2010, and that it will cost at least an additional 80 million dollars to develop and test [28].

Secure Flight was introduced shortly after the agency abandoned plans for its predecessor, the second generation Computer Assisted Passenger Prescreening System (CAPPS II). This scheme would have examined commercial and government databases to assess the risk posed by each passenger [22, 57]. CAPPS II was scheduled for a test run in the spring of 2003 using passenger data to be provided by Delta Airlines. Following a public outcry, however, Delta refused to provide the data and the test run was delayed indefinitely [16].

Having one's name on the no-fly list can be extremely dangerous. On September 26, 2002, Maher Arar, a Canadian software engineer changed flights in New York en route from Tunis to Montreal. He was detained by the United States Immigration and Naturalization Service, after his name came up in a database search due to misleading information supplied by the Royal Canadian Mounted Police. Even though he carried a Canadian passport, Arar was flown to Syria, against his will, where he was held in solitary confinement for over a year, and tortured regularly. After a year, the Syrian government concluded that he had no terrorist links and sent him back to Canada. Arar received a full apology from the Canadian Prime Minister in 2007, and received over 10 million dollars in compensation [29]. The US government insists that he has terrorist links, and has refused repeated requests from the Canadian government to remove him from the no-fly list.

Arar's experience highlights the most extreme consequences of appearing on the no-fly list. His experience and the more common experiences of passengers being delayed, detained or arrested [32], demonstrate the reasons why someone may want to evade an error prone watchlist plagued with false positives. However, the techniques for evading the no-fly list outlined in this paper are solely for domestic flights, and so even if he had known about them, Mr Arar would have been unable to use them.

2 Flying Without Identity Documents

There is no law or official regulation which requires that passengers show any identity document to a US government employee in order to board an airplane [44, 43]. TSA encourages travelers to have a government issued photo ID ready for inspection, yet its website does acknowledge an alternative option, stating that "the absence of proper identification will result in additional screening" [55]. TSA has repeatedly refused passengers' requests for the regulations detailing the ID policy. The government asserts that the rules are classified as Sensitive Security Information [25, 6], and are thus free from any requirement to be made public. This refusal prompted activist John Gilmore to file a lawsuit, which subsequently lead to the US Court of Appeals (9th Circuit) looking at the policies *in camera*. The judges summarized the policies in question, and thus, in theory, the right to fly without any ID in their opinion in *Gilmore v. Gonzales*, stating [18]:

> The identification policy requires that airline passengers either present identification or be subjected to a more extensive search. The more extensive search is similar to searches that we have determined were reasonable and consistent with a full recognition of appellants constitutional right to travel.

Passengers may be required to show identification to airline staff, but that is a private contractual matter between passengers and the airline. As such, the requirements tend to vary from airline to airline, based on their particular corporate policies [11, 10]. Through a combination of first-person testing by a number of activist passengers around the country [58, 33, 44, 56] and tests we have personally conducted, we have been able to piece together a picture of the ID requirements of a number of US airlines. Passengers have been able to successfully board domestic flights in the United States on multiple

airlines, including Northwest and United [45, 49], all without a single piece of identification. Other airlines require *some* form of identification. Passengers have been able to board flights on Continental, Delta and American Airlines with identity documents that include: prepaid credit cards purchased in cash, a library card and a hand-laminated membership card to a local organic supermarket [47, 48, 56]. Passengers typically have few if any problems when they claim to have forgotten their ID. However, passengers who attempt to assert their right to fly without ID have at times, met stiffer resistance from TSA [46, 30].

2.1 Interacting With The Airlines

Passengers are only required to interact with airline check-in staff when they wish to "check" a bag - and have the airline take care of their luggage for them. If a passenger is content to fly with just "carry on" items, she can quite easily make her way past the TSA checkpoint and only ever encounter airline staff at the gate, before boarding the airplane.

Any passenger that wishes to fly without approved identification documents must be in possession of a boarding pass marked with the letters "SSSS" (Secondary Security Screening Selectee), which instructs TSA staff to perform a more vigorous, or secondary search on the passenger. On some airlines, check-in staff can use their computer terminals to print out special boarding passes that have the letters "SSSS" printed on them [48, 45]. Other airlines simply have staff write the letters "SSSS" on the boarding passes with an ink marker [47].

If a passenger approaches a TSA checkpoint without the approved identification documents, and without a specially marked boarding pass, TSA are supposed to turn the passenger away, and instruct them to obtain a special boarding pass from the airline [47]. The legal hazards of testing the system have prevented us from attempting to go through a TSA checkpoint with a self-marked boarding pass - and so, we cannot conclusively state that a passenger is able to do this. However, in addition to successfully flying a number of times with "SSSS" boarding passes hand marked by airline staff, we have also successfully gone through security with a boarding pass incorrectly marked by the airlines: "SSS" instead of "SSSS", all without a single problem [47]. TSA staff have no way of knowing who wrote the letters "SSSS" on a boarding pass. This is mainly due to the fact that it is a hand-writen addition to the boarding pass, which could be added by any one of the hundreds of check-in employees who work at each airport. There is not even an attempt to document the source of the "SSSS", through the use of an employee's signature, initials or name.

If a nefarious passenger whose name appears on the no-fly list wishes to fly, the simplest way for her to successfully board an airplane would be to purchase a ticket in a fake name. If the passenger has booked a ticket on an airline that is relatively friendly towards passengers that do not have ID, she should be able to claim forgotten ID and request an "SSSS" boarding pass. If the passenger happens to be flying on an airline with stricter rules, it may be more effective to print out a boarding pass at home, and then hand-write the letters "SSSS" onto the boarding pass in a red ink pen - unless she is willing to go through the trouble of procuring a fake library or student ID card with which to prove her false identity to the airline. The passenger will be thoroughly

screened by TSA, and eventually allowed to board the plane. If her only goal is to evade the no-fly list, this simple technique should result in success.

We are not aware of any passenger who has successfully flown on a ticket purchased in a fake name, because testing this vulnerability may be illegal. However, a number of passengers have documented their experiences flying within the United States without showing a single piece of identification at the airport [49, 44]. Therefore, while we cannot state with the confidence that comes only through careful experimentation that this method of subverting the no-fly list is possible, it logically follows that it would.

3 Print-At-Home Passes

There are three varieties of boarding passes used by airlines. Those printed by airline check-in/gate staff, on official airline cardstock, those printed by unsupervised passengers using self-service check-in machines, and those printed out at home by passengers. This third type of boarding passes is the primary focus of this paper. It is quite possible that someone could make fraudulant tickets on couterfeit cardstock. With the help of an insider, it is also possible to produce documents on official airline stationary that listed fake information. Both of these threats are outside of the scope of this paper.

Print-at-home boarding passes were first introduced by Alaska Airlines in 1999, and have been in use by most US airlines since 2003. Usage rates vary by airline - as of 2006, 5 percent of eligible passengers on Delta Airlines print their boarding passes online, 9 percent at US Airways, 11 percent at NorthWest Airlines, and 15 percent usage amongst AirTran passengers [3]. Print-at-home boarding passes are much favored by both airlines and business travelers, their most frequent and profitable customers. A business passenger who has already printed out her own boarding pass and who is only traveling with carry-on baggage does not need to interact with airline staff until she has her pass scanned as she boards the airplane. This saves the airline a significant amount of money in labor and overhead costs, cuts down on average check-in time for other passengers who do require the help of an airline staff member, and reduces the amount of time that it takes for travelers to get through the airport and onto the airplane.

The online check-in process enables a passenger to login to the airline's website up to 24 hours before the flight, select seating, request an upgrade, enter their frequent flier number, and then finally, print out a dual human/machine-readable document - typically a combination of text, images and a barcode - from the comfort of their own home. Southwest Airlines famously does not allow passengers to reserve seats ahead of time, but allows passengers who check-in online to be amongst those who board the plane first, and thus get a chance at a window or aisle seat [27]. In an effort to further target business passengers, some airlines enable passengers to receive their boarding passes by fax [12, 34].

3.1 A No-Fly List Oracle

Most passengers can check-in online and print out their own boarding passes. International passengers are not able to print out their boarding passes at home, due to the legal requirement that airlines fully check their identity documents and verify that they have

the necessary visa or passport to enter their destination country. While the airlines have a significant amount of flexibility for domestic passengers who lose or forget their ID, the rules for international passengers are far more strict.

Any domestic passenger whose name matches an entry in the no-fly list will be denied the option of printing a usable boarding pass at home [54]. Similarly, passengers who have been selected by the airline's computer systems for additional screening — due to the purchase of a one way ticket, a ticket paid in cash or a number of other suspicious behavior based triggers — will also need to present themselves to an airline staff member at the airport in order to obtain a valid boarding pass.

Researchers have previously noted that predictability in airport security systems is far worse than random searching. By traveling multiple times in advance of an attack, would-be terrorists can determine whether they are subject to different treatment. Those who are not selected for additional screening can be assigned to act. This ability to safely probe the watch lists through the use of "dry-runs" enables attackers to learn who amongst their team are likely to set off any passenger screening system alerts, all without jeopardizing their mission, or even risking jail [9]. Likewise, the ability to check-in online creates an easy to use oracle for learning who is and is not on the no fly list, from the comfort and safety of an anonymized Internet connection [14], a public library, or Internet cafe.

To verify if a name is or is not on the no-fly list, one can do the following:

1. Purchase a fully refundable ticket online in the name which one wishes to verify against the no-fly list (the subject).
2. Purchase a fully refundable ticket online in the name of a passenger who has recently flown without any problems (the control).
3. Attempt to check-in online less than 24 hours before the flight for both passengers.
4. Call the airline to cancel both tickets, and ask for a refund.

If one is able to successfully print out a valid boarding pass in the name of the control, but not the subject, it is quite likely that the subject's name is on the no-fly list. If, however, both passengers are denied the ability to print out a boarding pass online, it is far more likely that some other factor is triggering one of the secondary-screening rules.

4 Boarding Pass Systems

The airlines each employ differing and incompatible systems for the production and printing of online boarding passes. A large percentage of them do share at least one common property: They present the user with a html web page that contains all of the pertinent portions of the passenger record - first and last name, flight number, departure and destination cities, date, gate, etc - all in plain text, which can be saved and edited after the fact if a computer savvy user chooses to do so. Such passes typically include a handful of images. These include the airline's name or logo, and a computer readable barcode that will be scanned at the gate before the passenger boards the flight. Other airlines present the user with a single file, which contains all of the boarding pass

information embedded in a single image. While this can also be modified with a graphical editing program such as Adobe Photoshop, it does require more effort and skill to modify than a text based html document [7].

Even when an airline produces a single-image based boarding pass, it is still possible for a motivated and technically skilled person to create a html based, and thus easily modifiable boarding pass that can pass for a real one. The goal of the attacker is typically not to produce a document that is 100% identical to the real article and able to withstand analysis by a trained forensics expert. It is rather to produce one that is good enough to pass the cursory check performed by a TSA employee, who sees several hundred similar documents every day.

The simplest method of producing a fake boarding pass is to use the html web page that the airline returns upon completion of online check-in. By saving this document locally, a user has everything she needs to produce documents good enough to get past current TSA checkpoints. Multiple websites have been created that automate this process, and allow anyone to print out a completely customizable yet authentic looking boarding pass. One of the sites was publicly shut down by the FBI (see figure 1) [23], while another remains online [1].

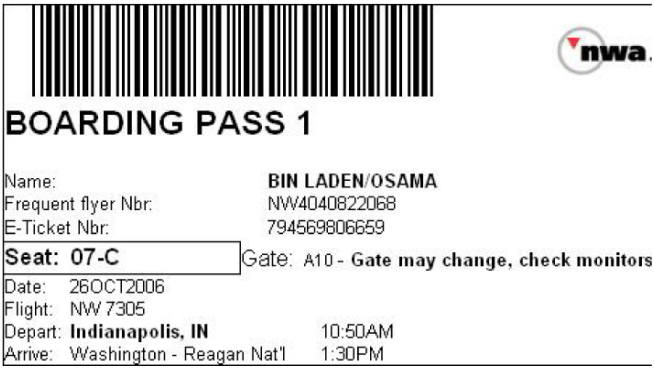

Fig. 1. A fake boarding pass created by a now shut-down website.

Bruce Schneier was the first to alert the public to this loophole in August of 2003. Since then, a number of commentators have written about the problem and all provide detailed instructions describing the process necessary to modify a print-at-home boarding pass [38, 3, 7, 39]. In particular, Senator Charles Schumer of New York has on multiple occasions provided step-by-step instructions for doing this on his official senate web site [40, 41].

Although these methods will allow someone to create a boarding pass good enough to get past security, the barcode included on each of these documents refers to a specific booking in the airline's reservation system. Any future attempted reuse of this barcode in a fake document will result in an invalid boarding pass, at least when presented to the airline employees at the gate. A passenger can get past the TSA checkpoint with

one of these documents, as screening staff do not have the ability to access live passenger records, but it will not be enough to get aboard an airplane. To achieve that goal, a passenger whose name is on the no-fly list can use the combination of a genuine print-at-home boarding pass (purchased in a false name) with a fake boarding pass prepared at home. More importantly, she can do so while presenting her real identification documents, and will be able to avoid the rigorous and extensive screening procedures required when a passenger declines to show identification documents, as outlined earlier in this paper. Senator Schumer's instructions clearly explain this process [40]:

1. Joe Terror (whose name is on the terrorist watch list) buys a ticket online in the name of Joe Thompson using a stolen credit card. Joe Thompson is not listed on the terrorist watch list.
2. Joe Terror then prints his Joe Thompson boarding pass at home, and then electronically alters it (either by scanning or altering the original image, depending on the airline system and the technology he uses at home) to create a second almost identical boarding pass under the name Joe Terror, his name.
3. Joe Terror then goes to the airport and goes through security with his real ID and the FAKE boarding pass. The name and face match his real drivers license. The airport employee matches the name and face to the real ID.
4. The TSA guard at the magnetometer checks to make sure that the boarding pass looks legitimate as Joe Terror goes through. He/she does not scan it into the system, so there is still no hint that the name on the fake boarding pass is not the same as the name on the reservation.
5. Joe Terror then goes through the gate [onto] his plane using the real Joe Thompson boarding pass for the gates computer scanner. He is not asked for ID again to match the name on the scanner, so the fact that he does not have an ID with that name does not matter. [Since Joe Thompson doesnt actually exist, it does not coincide with a name on the terrorist watch list] Joe Terror boards the plane, no questions asked.

4.1 A Denial Of Service Attack Against The Transportation Security Administration Screening Process

In addition to enabling passengers to circumvent the no-fly list, the modifiable print-at-home boarding pass vulnerability can be used as an attack vector for other nefarious activities. Byers et. al. originally introduced the idea of an Internet-based attack against physical world resources in 2002 [8]. We now propose a similar attack against the TSA checkpoints at airports. Due to the significant legal risks involved in implementing this idea, we are unable to produce a proof-of concept. We are, however, able to explain it in some detail.

Every passenger whose boarding pass lists the letters "SSSS" is sent for secondary screening. Typically, their carry-on bags are emptied, searched, swabbed for chemical analysis, and in general, they are subjected to a significantly higher level of scrutiny than a typical passenger. They will also often be required to go through a physical pat-down by a TSA employee after walking through a magnetometer and or a chemical "puffer" machine. This experience commonly takes up to 10 minutes of at least one TSA agent's time, if not multiple agents.

The attack we propose requires a malicious software payload, which can be executed as a covert web-browser extension. This can be implemented using the Firefox Greasemonkey framework [37], or similar technologies for Microsoft Internet Explorer. Such a program will modify each html print-at-home boarding pass to add the letters "SSSS" to the pass in a highly visible place. There are a small enough number of domestic airlines in the Unites States that hard-coding the web site address of each airline's print-at-home boarding pass web page into a virus payload will not be too difficult. The technique will be particularly effective if it spreads across corporate networks, and worse, the public computer terminals at hotels used by business travelers.

Such a system will essentially force every infected passenger to be sent through an additional screening process. If distributed to enough computers, this will result in either significantly longer lines at the checkpoints and or significantly less attention being spent on each passenger undergoing the secondary screening process. The entire "SSSS" process is shrouded in such secrecy that passengers have no way of knowing if they will be selected under normal circumstances. It is therefore highly unlikely that travelers will associate their invasive search and delays at the airport with a potential software infection on their computer.

4.2 Boarding Pass Failures

Currently, the airlines are responsible for comparing a passenger's name against the government provided no-fly list. TSA must assume that if a passenger is in possession of a valid looking boarding pass, that their name has been compared against this list. If boarding passes can only be printed out by an airline employee after checking the ID of the passenger, the system remains reasonably secure. The no-fly list's integrity can be maintained even after the introduction of user-printed boarding passes, as long as the airlines compare each user's identity documents at the gate - and check ID's against the reservation in their computer system. Immediately after the September 11th 2001 terrorist attacks, this additional verification step was introduced. However, this check was later removed after complaints from the airlines that it caused additional delays to the boarding process [5].

When a passenger goes through a TSA checkpoint, several events occur. Assuming that the passenger presents some form of ID, TSA staff will compare the name on the ID to the name on the boarding pass. They will also check the time and date, departure airport name, and the terminal number. Staff will typically mark the boarding pass with an ink pen to certify that the passenger's identification documents have been checked. Other than by looking at the document, TSA employees have no way of verifying if the the boarding pass is real, valid, has been photocopied and used already that day or if it has been tampered with or modified by the would-be passenger.

TSA does not currently collect much data, if any at all. This is due to the fact that passenger's names are not recorded, nor is any information kept on the kind of identification presented. If asked after the fact, TSA will probably not be able to produce records listing when the passenger arrived at the checkpoint or how long it took to go through the checkpoint. If a checked-in passenger walks out of the airport 10 minutes before the plane departs, TSA will not know until the airline notifies them when their passenger count comes up short. This information may be obtainable after the

fact through analysis of security camera tapes, but only if the authorities have a means of matching a face on film to a passenger record. It will certainly not be available in real-time.

5 Fixing The Problems

In response to the significant press coverage in the last year over the issue of fake boarding passes [23, 53], some commentators suggested that TSA should be given the means to check passengers' ID against the airlines' computer systems. Others continued to call for the airlines to restart the now-discontinued practice of checking ID's at the gate, a process that is still performed in Europe and elsewhere [42, 7, 41]

While having the airlines perform an ID check at the gate is the easiest solution to the main problem of user modified boarding passes, it does nothing to defend against the physical denial of service attack introduced earlier in this paper. In any case, it is a moot point, as the airlines clearly do not wish to bear the costs associated with an additional ID check before boarding. Thus, we now explore two alternative schemes that neutralize the modified boarding pass threat, the physical denial of service attack, allow TSA to perform the no-fly list check themselves as passengers pass through security, and enable the government to collect a wealth of live data on users as they pass through the security checkpoints.

Both schemes involve equipping TSA employees with handheld wireless devices, which are able to scan or photograph the barcodes printed on passengers' boarding passes.

5.1 A Naive Fix

The first solution requires that the airlines provide TSA with live access to their Passenger Name Record databases. Either the airlines will be required to agree upon a common data export standard, and therefore devote the resources required to modify their systems to use such a standard, or TSA will have to develop a system that can interface with each airline's unique database. Likewise, the airlines will either need to move to a common barcode standard for their boarding passes, or TSA will have to create software that can read the differing barcode schemes used by each airline. In addition to this time consuming and thoroughly expensive development process, the airlines will also have to expend significant resources to provide constant, live and secure access to their databases.

5.2 An Improved Fix

The main goal of a boarding pass verification system is to make it impossible to pass through the security checkpoint with a fake or modified boarding pass. There is no real need to give TSA live access to the airline's databases. TSA employees merely need a way of verifying that the boarding pass presented to them is valid and has not been modified in any way.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (GNU/Linux)
Comment: See http://www.kernel.org/
signature.html for info

iD8DBQA/5WgqyGugaIF9Dw4RAjIiAJ0bz3q
+NGPPol3KTQ/NOVz8djN5+ACdEyvx
u1MeKSNl+5pOBjFxv63JPHk==CX+2i

-----END PGP SIGNATURE-----

Fig. 2. An OpenPGP signature encoded as a QRcode

In 2002, Lee et al. introduced the idea of using dense 2D barcodes to store digital signatures. They used the QRcode 2D matrix scheme (see figure 2), which can store up to 2,953 bytes of data per barcode. With current printing and reader technology, a 1024 bit signature can be printed in an area less than 10 mm sq [26]. The QRcode technology is already widely deployed in Japan. Barcodes are embedded in advertising posters, billboards, magazines and even fast food wrappers [51]. Most mobile phones on the Japanese market now include software that can scan the barcode using the built in camera phone. The barcode scheme is a clearly defined standard, with open source software development kits available as well as free, ready-to-use readers for Symbian OS and Java mobile phone devices [21].

We propose to embed all of the information typically printed on a boarding pass, along with a digital signature in a QRcode matrix. This can be produced by a software kit given to each airline. As all of the information to be contained in the barcode is already available at the time that the boarding pass is printed by the user, it should not require a significant engineering effort to use that same information to generate the barcode. There are a small enough number of domestic carriers in the United States that TSA can require each airline provide it with their barcode public key - and thus the airlines will simply self-sign their boarding pass barcodes. This negates any need for a central Public Key Infrastructure.

TSA personnel can thus be issued with a hand-held wireless computing device, capable of taking a photo of the barcodes. Screening staff will scan each 2D barcode-enabled boarding pass, after which, the software on the device will verify all of the information contained in the barcode, and using the public key given to TSA by the airline, will be able to verify that none of the information in the barcode has been tampered with or in any way modified since the barcode was produced.

All of the information needed to verify a boarding pass' authenticity is currently made available by the airlines at the time of boarding pass creation, so that the document can be printed out. No new information will be required of them. Thus, they are immediately freed of the requirement of providing live access to their databases to TSA.

If required, the airlines can publish a revocation list of the boarding passes that are no longer valid. Since boarding passes can only be printed at home within 24 hours of departure, it is quite likely that this list will remain rather small. The airlines can publish such a revocation list on their websites, or through some other public means, without risking any private passenger data, by only listing a unique barcode number associated with each boarding pass.

6 Improvements and Passenger Tracking

In both of these proposed schemes, TSA employees will be equipped with hand-held devices that scan the barcode on a boarding pass, and will display the passenger's information on the device's screen. By comparing the data on the screen (which will either be from the airline's database, or stored in the barcode and signed by the airline as original and unmodified) with the information on the passenger's identity documents, TSA agents will be able to completely do away with the threat of passenger modified boarding passes, as well as the risk posed by the physical denial of service attack introduced earlier in this paper. This is because TSA staff will not rely on the text printed on the boarding pass to learn a passenger's name, flight information and secondary screening status. They will instead be able to depend on a live database record or a digitally signed barcode to provide them with a trustworthy copy of that information.

As TSA agents will now have the passenger's name in a digital format as they go through the security checkpoint, it will be possible for TSA to take over the task of performing the no-fly list searches themselves. This will increase the security of the list, as it will no longer have to be shared with the airlines and will only be accessible by federal employees. Likewise, this will neutralize the at-home method of querying the no-fly list outlined in section 3.1 of this paper, as passengers will no longer be inadvertently told during online check-in if they are on the no-fly list or not.

Depending on the time required to query the no-fly list, the search can either happen as soon as the barcode is scanned, or, if more time is needed, the passenger's boarding pass can be scanned twice: once upon entering the security line — where the name will be read and submitted to a central database for comparison — and again once the passenger has passed through the metal detector, where the results of the search can be viewed to see if the passenger will be allowed to continue.

Many state drivers licenses already include information on the back of the license in a machine readable format, typically a barcode [13]. Were it required, such functionality can be added to TSA's hand-held devices, thus further reducing the amount of work that TSA staff are required to perform, and consequently, the possibility of human-related error. It is quite easy to imagine a scenario where a TSA employee scans the barcodes on the boarding pass and on the back of the passenger's drivers license, waits a few seconds as the system compares the passenger's name to the no-fly list, and then allows the passenger to pass after the system displays a message instructing the employee that the passenger is clear to fly.

In addition to simply checking a passenger's name against the no-fly list, TSA will now have a significant tool with which to collect real time data on passenger movement through airport terminals. They will be able to collect data on how long passengers

arrive before their flights, how long it takes to get through the security checkpoint, assuming that the ID/pass is checked upon entering the line, and then again after the passenger goes through the magnetometer. Given that many state governments have monetized their drivers license databases [50, 15], it does not seem completely unrealistic to imagine a scenario where TSA will provide some of this data for sale. Airline food and concession vendors will probably be a fantastic market and would probably be very interested to know how long passengers spend captive in the airport, waiting for their flight to leave.

In the case that passengers are flying without ID, this system will at least enable TSA to lock a specific passenger ticket number as "used", and thus forbid multiple passengers without ID from passing through the checkpoint with a photocopy of the same print-at-home boarding pass. Were TSA to require that passengers leaving the secure area have their boarding passes scanned, this will also provide a key data source on the few passengers who leave the airport after clearing security, instead of boarding the flight. No doubt, TSA will probably like to identify and then question these passengers to discover the reason they were doing this, something that is not possible under the current system.

It is important to note that the system described in this paper will only fix the problem of fake or modified boarding passes. Even if TSA staff are equipped with hand-held devices, passengers will still be able to decline to show ID, and thus evade the no-fly list. This is not a problem that technology can solve, but is something that the US government must fix through policy changes, if it really wishes for a no-fly list to exist, and to be effectively enforced.

7 Conclusion

In this paper, we have outlined several problems with the enforcement and application of the no-fly list to domestic passengers in the United States. One of these problems is due to the fact that passengers can legally fly without showing any identity documents to US government employees, and can often fly without showing any such papers to airline staff. This problem remains open, and cannot be fixed without a change in policy by the US government.

We have also highlighted the problem of fake or user modified boarding passes, a problem which has been known, yet largely ignored by the government for a number of years. This issue has recently been the subject of a significant amount of press coverage, but as of now, remains unfixed. We introduced a method of determining if any particular name is on the no fly list, which one can perform safely and anonymously over the Internet. We introduced a physical denial of service attack against the TSA checkpoints at airports, distributed via an Internet virus.

We proposed two solutions to these problems, one naive yet expensive for the airlines, and another solution that retains many of the same security properties of the first, yet which is significantly cheaper. This second solution also frees the airlines of the costly and complicated need to provide live access to their passenger databases.

Both of these solutions will give TSA access to a wealth of live data on passengers activity in the airports, from the number of passengers at a particular checkpoint, the

amount of time it takes a particular passenger to get through a checkpoint, to the amount of time a passenger waits in the departure area before boarding their flight. More importantly, both of the proposed solutions make the use of fake or modified print-at-home boarding passes impossible and will provide TSA with a means to check passenger's names against the no-fly list at the time they pass through security checkpoints.

Acknowledgements

Many thanks to Kelly Caine, John Doyle, Virgil Griffith, Kristin Hanks, Markus Jakobsson and Katherine Townsend for their helpful comments. Sid Stamm provided both helpful feedback and helped to flesh out the idea of the boarding pass virus discussed in section 4.1.

References

1. John Adams. Document gennreator [sic], November 1 2006. http://j0hn4d4m5.bravehost.com/.
2. American Civil Liberties Union. Frequently Asked Questions About the "No Fly List", October 26 2005. http://www.aclu.org/safefree/general/21164res20051026.html.
3. Anonymous. Airport Security's Achilles' Heel. *CSO: The Resourcec for Security Executives*, February 01 2006. http://www.csoonline.com/read/020106/caveat021706.html.
4. Associated Press. TSA's Secure Flight program suspended, February 09 2006. http://www.msnbc.msn.com/id/11254968/.
5. Matt Blaze. Human-scale security and the TSA, January 01 2007. http://www.crypto.com/blog/tsa_paranoia.
6. Sara Bodenheimer. Super Secret Information? The Discoverability Of Sensitive Security Information As Designated By The Transportation Security Administration. *UMKC L. Rev.*, 73:739, Spring 2005.
7. Andy Bowers. A dangerous loophole in airport security. *Slate Magazine*, February 07 2005. http://www.slate.com/id/2113157/.
8. Simon Byers, Aviel D. Rubin, and David Kormann. Defending against an internet-based attack on the physical world. *ACM Trans. Inter. Tech.*, 4(3):239–254, 2004.
9. Samidh Chakrabarti and Aaron Strauss. Carnival booth: An algorithm for defeating the computer-assisted passenger screening system. *First Monday*, 7(10), 2002. http://firstmonday.org/issues/issue7_10/chakrabarti/index.html.
10. Jayen Clark. Just who do you think you are, without ID? *USA Today*, April 28 2005. http://www.usatoday.com/travel/news/2005-04-28-travel-ids_x.htm.
11. Continental Airlines. ID Requirements, 2007. http://www.continental.com/web/en-us/content/travel/airport/id/default.aspx.
12. Continental Airlines. Online Check-in FAQ, 2007. http://www.continental.com/web/en-US/content/help/onlinecheckin.aspx.
13. John T. Cross. Age Verification In The 21st Century : Swiping Away Your Privacy. *John Marshall J. of Comp. & Info. Law*, 23(2), Winter 2005.
14. Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004. http://tor.eff.org/tor-design.pdf.

15. Serge Egelman and Lorrie Faith Cranor. The Real ID Act: Fixing Identity Documents with Duct Tape. *I/S: A Journal of Law and Policy for the Information Society*, 2(1):149–183, Winter 2006.
16. Electronic Privacy Information Center. EPIC Secure Flight Page, February 09 2006. http://www.epic.org/privacy/airtravel/secureflight.html.
17. Justin Florence. Making The No Fly List Fly: A Due Process Model For Terrorist Watchlists. *Yale Law Journal*, 115(8):2148–2181, June 2006.
18. *Gilmore v. Gonzales*. 04-15736 (9th Cir. 2006). http://www.papersplease.org/gilmore/_dl/GilmoreDecision.pdf.
19. Jim Harper. *Identity Crisis: How Identification Is Overused and Misunderstood*, chapter 23, page 215. CATO Institute, Washington, DC, 2006.
20. Kip Hawley. Prepared statement. *U.S. Senate Committee on Commerce, Science and Transportation*, January 17 2007. http://www.tsa.gov/press/speeches/air_cargo_testimony.shtm.
21. Kaywa Reader. What is the Kaywa Reader, 2006. http://reader.kaywa.com/faq/25.
22. Leigh A. Kite. Red Flagging Civil Liberties and Due Process Rights of Airline Passengers: Will a Redesigned CAPPS II System Meet the Constitutional Challenge? *Wash. & Lee L. Rev.*, 61(3), Summer 2004.
23. Brian Krebs. Student Unleashes Uprorar With Bogus Airline Boarding Passes. *The Washington Post*, November 1 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/10/31/AR2006103101313.html.
24. Steve Kroft. Unlikely terrorist on no fly list. *60 Minutes*, October 8 2006. http://www.cbsnews.com/stories/2006/10/05/60minutes/printable2066624.shtml.
25. Linda L. Lane. The Discoverability of Sensitive Security Information in Aviation Litigation. *Journal of Air Law and Commerce*, 71(3):427–448, Summer 2006.
26. Jaeil Lee, Taekyoung Kwon, Sanghoon Song, and JooSeok Song. A model for embedding and authorizing digital signatures in printed documents. In *ICISC*, pages 465–477, 2002.
27. Ron Lieber and Susan Warren. Southwest Makes It Harder To Jump the Line. *The Wall Street Journal*, June 7 2006. http://online.wsj.com/article/SB114964168631673304.html.
28. Eric Lipton. U.S. Official Admits to Big Delay in Revamping No-Fly Program. *The New York Times*, February 21 2007. http://www.nytimes.com/2007/02/21/washington/21secure.html.
29. Andrew Mayeda and Sheldon Alberts. Harper offers Arar apology – and $10M. *The Star Phoenix*, January 27 2007. http://www.canada.com/saskatoonstarphoenix/news/story.html?id=441709d5-8eea-4588-ab00-902b748408d2.
30. Declan McCullagh. Airport ID checks legally enforced? *CNET News.com*, December 8 2005. http://news.com.com/Airport+ID+checks+legally+enforced/2100-7348_3-5987820.html.
31. Leslie Miller. Report: Thousands Wrongly on Terror List. *The Associated Press*, October 6 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/10/06/AR2006100601360.html.
32. Mima Mohammed and Jenny Allen. Grad files national suit. *The Stanford Daily*, February 16 2006. http://daily.stanford.edu/article/2006/2/16/gradFilesNationalSuit.
33. Eric Nguyen. No ID, June 12 2006. http://mindtangle.net/2006/06/12/no-id/.

34. Northwest Airlines. Press Release: Northwest Expands Boarding Pass Faxing Service to International Locations, October 19 2006. http://news.thomasnet.com/companystory/496855.
35. Yousri Omar. Plane Harassment: The Transportation Security Administration's Indifference To The Constituion In Administering The Government's Watch Lists. *Wash. & Lee J. Civil Rts. & Soc. Just.*, 12(2), Spring 2006.
36. Soumya Panda. The Procedural Due Process Requirements for No-Fly Lists. *Pierce L. Rev.*, 4(1), December 2005.
37. Mark Pilgrim. What is greasemonkey, May 9 2005. http://diveintogreasemonkey.org/install/what-is-greasemonkey.html.
38. Ryan. Changing A Southwest Boarding Pass, July 30 2006. http://boardfast.blogspot.com/2006/07/how-to-change-southwest-airlines.html.
39. Bruce Schneier. Flying on Someone Else's Airplane Ticket. *Crypto-Gram*, August 15 2003. http://www.schneier.com/crypto-gram-0308.html#6.
40. Charles Schumer. Schumer reveals new gaping hole in air security, February 13 2005. http://www.senate.gov/~schumer/SchumerWebsite/pressroom/press_releases/2005/PR4123.aviationsecurity021305.html.
41. Charles Schumer. Schumer Reveals: In Simple Steps Terrorists Can Forge Boarding Pass And Board Any Plane Without Breaking The Law!, April 09 2006. http://www.senate.gov/~schumer/SchumerWebsite/pressroom/record.cfm?id=259517.
42. Adam Shostack. On Printing Boarding Passes, Christopher Soghoian-style. Emergent Chaos, October 28 2006. http://www.emergentchaos.com/archives/2006/10/on_printing_boarding_pass.html.
43. Ryan Singel. Fliers can't balk at search. *Wired News*, March 20 2006. http://www.wired.com/news/technology/1,70450-0.html.
44. Ryan Singel. The Great No-ID Airport Challenge. *Wired News*, June 9 2006. http://www.wired.com/news/technology/0,71115-0.html.
45. Christopher Soghoian. Slight Paranoia: TSA Love, September 21 2006. http://paranoia.dubfire.net/2006/09/tsa-love.html.
46. Christopher Soghoian. ID rules inna Babylon: A police confrontation at DCA Airport, February 19 2007. http://paranoia.dubfire.net/2007/02/id-rules-inna-babylon-police.html.
47. Christopher Soghoian. Slight Paranoia: A clearer picture of how to fly with no ID, January 21 2007. http://paranoia.dubfire.net/2007/01/clearer-picture-of-how-to-fly-with-no.html.
48. Christopher Soghoian. Slight Paranoia: Much fun at SFO airport, January 29 2007. http://paranoia.dubfire.net/2007/01/much-fun-at-sfo-airport.html.
49. Christopher Soghoian. Slight Paranoia: No ID on United: Piece of Cake, February 02 2007. http://paranoia.dubfire.net/2007/02/no-id-on-united-piece-of-cake.html.
50. Daniel J. Solove. Access And Aggregation: Public Records, Privacy And The Constitution. *Minn. L. Rev.*, 86:1137, June 2002.
51. Spark Productions. Japanese QR codes provide marketers a glimpse of the future. *Japan Marketing News*, January 17 2007. http://www.japanmarketingnews.com/2007/01/in_previous_art.html.
52. Daniel J. Steinbock. Designating The Dangerous: From Blacklists To Watch Lists. *Seattle Univerity Law Review*, 30(Issue 1), Fall 2006.
53. Randall Stross. Theater of the Absurd at the T.S.A. *The New York Times*, December 17 2006. http://www.nytimes.com/2006/12/17/business/yourmoney/17digi.html.

54. Transportation Security Administration. TRIP: Traveler Identity Verification Form, February 20 2007. https://trip.dhs.gov/.
55. Transportation Security Administration. TSA: Our Travelers: What you need, February 13 2007. http://www.tsa.gov/travelers/airtravel/screening/index.shtm#5.
56. Siva Vaidhyanathan. Can you board a plane without ID?, March 24 2006. http://www.nyu.edu/classes/siva/archives/002939.html.
57. Deborah von Rochow-Leuschner. CAPPS II and the Fourth Amendment: Does It Fly? *Journal of Air Law and Commerce*, 69(1):139–173, Winter 2004.
58. David Wagner. Flying without ID, October 20 2000. http://www.cs.berkeley.edu/~daw/faa/noid.html.