Privacy Impact Assessment
for the

Boarding Pass Scanning System

November 29, 2007

Contact Point
Mike Golden
Assistant Administrator
Operational Process & Technology
Mike.Golden@dhs.gov

Reviewing Official
Peter Pietra
Director, Privacy Policy & Compliance
Transportation Security Administration
TSAprivacy@dhs.gov

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Boarding Pass Scanning System (BPSS) is a process and technology that validates the authenticity of the boarding pass at the TSA security checkpoint using 2-dimensional (2D) bar code readers and encryption techniques. The BPSS will display machine readable data from the boarding pass for confirmation against the human readable portions of the boarding pass to verify that the boarding pass is legitimate and has not been tampered with. Once confirmed, the displayed data will be deleted from the BPSS.

Introduction

The vulnerabilities associated with fake boarding passes are well-known. In the fall of 2006 a doctoral student at Indiana University created a website that enabled individuals to create fake boarding passes. This website garnered significant media attention, as it demonstrated how a known terrorist who is on the Watch or No-Fly List could use a fake boarding pass to gain access to the sterile area of the airport. Once inside the sterile area, the terrorist could use a real boarding pass acquired under an alias to board the plane.

In order to eliminate this vulnerability, the Transportation Security Administration (TSA) has begun to pilot new technologies that can identify fake or tampered forms of identification. TSA also has begun to consider ways to encode boarding passes with a security code that could ensure their authenticity. The BPSS is a process and technology that validates the authenticity of the boarding pass at the TSA security checkpoint using 2-dimensional (2D) bar code readers and encryption techniques. The BPSS will be compatible with any 2D barcode and can be used with paper boarding passes printed on a home computer via online check-in procedures, paper boarding passes printed by the airlines, or a paperless boarding passes that are sent to passengers' mobile devices such as cell phones, Blackberrys, or Personal Digital Assistants (PDA).

The overall objective of BPSS is to ensure that the barcoded data in boarding passes are not tampered with. This can be done simply and to a high degree of security using standard digital signature technology based on Public Key Infrastructure (PKI) standards. When generating the barcode data, the airline will create a hash[1] of the barcode data and then encrypt the hash with the airline's "Private Key". The use of a hash function plus encryption will allow TSA to confirm that the barcode was issued by the airline and that none of the information in the barcode (such as the passenger's name) has been tampered with.[2] The encrypted hash is then appended to the end of the data before converting this to a barcode. This will add an additional 172 characters (bytes) to the barcode using a 1024 bit key. TSA will work within the International Air Transport Association's (IATA) existing Resolution 792, which provides airlines with standards for use of 2D barcodes.

At the checkpoint the TSA barcode reader will use the airline's "Public Key" to decrypt the hash. This allows TSA to verify the identity of the airline that created the barcode. At a second level, the decrypted hash will be compared against the rest of the barcode data. This will allow TSA to detect if the data has been tampered with. It would be extremely difficult to falsify a boarding pass if this approach is taken. A

[1] A hash function is a reproducible method of turning some kind of data into a (relatively) small number which identifies the data. The algorithm "chops and mixes" (i.e., substitutes or transposes) the data. The identifiers are called hash sums, hash values, hash codes or simply hashes. Hash sums are commonly used as indices into hash tables or hash files. Cryptographic hash functions are used for various purposes in information security applications.

[2] The hash function creates a unique alphanumeric sequence based on the data in the barcode. Any change in the data results in a change in the alphanumeric sequence generated by the hash.

passenger would need to modify the barcode data, regenerate the hash, and then encrypt this with the airline's private key. The only realistic way to achieve this is if the airline's private key was compromised. However, this is mitigated by installing a process where the private key is changed on a regular and random basis.

If a boarding pass is determined by the BPSS to have been tampered with or not authentic, the passenger will be referred to local law enforcement officers and TSA will capture the details of the incident in its existing incident database using established forms and processes. The primary database for capturing incident information at TSA is the Performance And Results Information System (PARIS).

Fair Information Principles

The Privacy Act of 1974 articulates concepts of how the Federal government should treat individuals and their information. These concepts are known as the Fair Information Principles (FIPs). The FIPs impose duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

As such, DHS has developed the Fair Information Principles that underlie the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The DHS Fair Information Principles account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. This PIA examines the privacy impact of BPSS operations as it relates to the Fair Information Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of Personally Identifiable Information (PII). Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

Most PIAs are conducted on IT systems that collect and retain PII. The BPSS does not use information in this way and, in fact, specifically does not retain any information once the boarding pass has been scanned. TSA is conducting this PIA in order to be further transparent and provide notice to the individual regarding the BPSS. Further, information on the BPSS will be posted to TSA's website.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Passengers will be aware that their ticket data will be collected and will have the opportunity to not

participate in this pilot by going through normal check-in procedures. When their information is collected, it is immediately displayed on the device screen, in order for TSA screeners to screen the passengers against their photo identification. Once this is completed, the information is immediately and permanently deleted from the system. Fundamentally, the BPSS merely electronically reads data that should be the same as what a human currently reads off the face of the boarding pass.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

TSA is responsible for security in all modes of transportation, including commercial aviation. 49 USC §114. Pursuant to that authority, as well as its general authorities to conduct research and development to enhance transportation security, TSA is evaluating the use of the BPSS as an improvement over current manual inspection of boarding passes by Transportation Security Officers (TSO). The PII embedded in the barcode of the boarding pass (including the passenger's name) will be momentarily captured by the BPSS to compare it to the data generated by the hash function. If the data matches, the passenger is cleared to proceed. Below is a table of all information contained in the barcode of the boarding pass that will be momentarily captured by the BPSS. "Mandatory data" is that data that is required to be in a bar code. "Conditional data" may be in the bar code depending on purchase conditions or preference of the airline.

MANDATORY DATA		CONDITIONAL DATA		
Unique	**Repeated**	**Unique**	**Repeated**	**For Individual Airline Use**
- Format Code (M) - Segment Count - Passenger Name - Electronic Ticket	- PNR/ Record Locator - From City Airport Code - To City Airport Code - Operating Carrier Code - Flight Number - Compartment Code - Seat Number - Check-in Sequence Number - Passenger Status	- Version Number - Passenger Description - Source of Check-in - Source of Boarding Pass - Date of Boarding Pass Issuance - Document Type - Airline Code of Boarding Pass Issuer	- Airline Numeric Code - Document Serial Number - Selectee Indicator - Int'l Document Verification - Marketing Carrier Code - Frequent Flyer Airline Code - Frequent Flyer Number - ID/AD Indicator - Free Baggage Allowance	- Bar Code Security

4. Principle of Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The BPSS temporarily displays to the human reader information contained in the barcode. The BPSS device application does not maintain a transaction log with bar code scan content; the application does not save or store the bar code scan data to a file, database, etc. When the user exits/closes the BPSS device application, the form closes. The memory (RAM) storing the scan data is released. When the BPSS device application is re-launched, the form is blank. Data from previous bar code scans is not displayed. When the user powers-off the device, any open applications are closed automatically. TSA does not collect or retain any

PII any longer than is necessary to confirm that the boarding pass is legitimate and has not been tampered with.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

None of the PII data collected by TSA through the BPSS will ever be disseminated or shared – not even within the Department. This data will be immediately deleted after it is compared with the hash. The memory is cleared once the next boarding pass is scanned.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

The PII collected for BPSS will be accurate, relevant, timely and complete in terms of airport information. This data will be checked for accuracy by utilizing a PKI hash function which will ensure non-repudiation of the data. If the data is incorrect or does not register with the BPSS device or the PKI hash cannot be validated, the TSO will be required to determine if the passenger requires secondary screening.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

All PII data collected by the BPSS devices will be collected in a manner that it is not saved on the device and is immediately deleted after being viewed by the TSO. Data from previous bar code scans is not retained or displayed. These devices employ security safeguards by not maintaining or keeping any PII data for longer than needed in order for the TSO to perform their job. Additionally, these devices will be locked down in accordance with DHS and TSA Security Requirements. The BPSS equipment is a handheld 2-D Bar Code scanning device and should be considered standalone as it will **not** be connected to any network - via wireless or ethernet connection.

When not in use the devices will be appropriately stored in secure locations under the supervision of the Federal Security Director.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Screeners and all personnel utilizing the BPSS devices will receive training. Additionally, these devices will be locked down according to DHS and TSA Security Requirements and will go through normal TSA Certification and Accreditation (C&A) and auditing processes.

TSA's operational integration team will perform operational testing and evaluation of the device to determine its efficacy and will develop a formal evaluation of the technology and supporting processes.

Conclusion

The BPSS will be a great asset to the TSA, as ultimately, it will enhance passenger security and the passenger experience in a number of ways. The PII that this system collects is not retained in any way on these devices and is of a very minimal risk to the passenger since only boarding pass information is collected. None of the PII data collected by TSA through the BPSS will be disseminated or shared – not even within the Department. This data will be immediately deleted after use.

Responsible Officials

Domenic Bianchini
Program Manager
Passenger Screening Program (PSP) Program Manager
Transportation Security Administration
Domenic.Bianchini@dhs.gov

Ely Kahn
Director, Risk Management and Strategic Innovation
Transportation Security Administration
Ely.Kahn@dhs.gov

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security