How to get good seats in the security theater?

Hacking boarding passes for fun and profit

Przemek Jaroszewski
przemj+defcon24@gmail.com
$ whoami

• head of Current Threat Analysis team at the Polish national CSIRT (CERT Polska)
• 10+ years of education in programming
• Master’s degree in social psychology
• 15 years of experience in IT security
• aviation enthusiast, unrealized air traffic controller
Up in the Air

• FF miles are nice, but status in nicer
Except when improvements don’t work...
Bar-Coded Boarding Pass

IATA Resolution 792

• Paper
  • PDF417

• Mobile
  • QR Code
  • Aztec
  • DataMatrix
Barcode Generator

Aislou  Tools

This app is compatible with all of your devices.

Installed

Create one of 11 types of codes

http://goo.gl/TnC-J94

Free (no ads, no special premissions) QR code / barcode generator,
You can create the following barcodes:
Where did we get?

• Free Fast Track for all travellers
M1 COLUMBUS/CHRISTOPHER E56 XXXX
WAWCPHSK 2762 666M009C0007 666>10B0
K6161BSK 25117999999153830 SK A3
1999999999 *3000500A3G
M1 COLUMBUS/CHRISTOPHER 56 YYYY
WA WCPH SK 2762 666 M 009 C 0007 6 66 > 10 B 0
K 6161 BSK 2511799999153830 SK A 3
1999999999 *3000500 A 3 G
Where did we get?

• Free Fast Track for all travelers
Wait, this is not news!

- Bruce Schneier (2003): Flying On Someone Else’s Airplaine Ticket
- Andy Bowers (2005): Dangerous Loophole in Airport Security
- Bruce Schneier (2006): The Boarding Pass Brouhaha
- Christopher Soghoian (2007): Insecure Flight: Broken Boarding Passes and Ineffective Terrorist Watch Lists
- Jeffrey Goldberg (2008): The Things He Carried
- Charles C. Mann (2011): Smoke Screening
No Fly List Bypass (in 2006)

• Buy tickets under false name
• Print your boarding pass at home
• Create a copy of the boarding pass with your real name
• Present the fake boarding pass and the real ID to TSA officers
• Present the real boarding pass to gate agents
• Fly
October 27, 2006

Mr. Christopher Coghoian
901 E. 10th Street
Bloomington, IN 47408

Dear Mr. Coghoian:

It has come to the attention of the Department of Homeland Security: TSA that you are currently operating a website which creates fraudulent airline boarding passes. The purpose of this letter is to notify you that your continued operation of this website may subject you to federal criminal penalties, including imprisonment and civil sanctions.

Title 18, United States Code, Section 1036 states:

Sec. 1036. Entry by false pretenses to any real property, vessel, or aircraft of the United States or secure area of any airport
(a) Whoever, by any fraud or false pretense, enters or attempts to enter--

(1) any real property belonging in whole or in part to, or leased by, the United States;
(2) any vessel or aircraft belonging in whole or in part to, or leased by, the United States; or
(3) any secure area of any airport, shall be punished as provided in subsection (b) of this section.

(b) The punishment for an offense under subsection (a) of this section is--

(1) a fine under this title or imprisonment for not more than 5 years, or both, if the offense is committed with the intent to commit a felony; or
(2) a fine under this title or imprisonment for not more than 6 months, or both, in any other case.

Title 49, United States Code, Section 46314 states, in part:

Sec. 46314. Entering aircraft or airport area in violation of security requirements
No Fly List Bypass (in 2016 Europe)

- Buy tickets under false name
- Print your boarding pass at home
- Fly

Impacting factors:
- Particular airline’s business consciousness
- Temporary security checks
So... Where is passenger data stored?

- Computer Reservation Systems (CRS) allow for storage and processing of Passenger Name Records (PNR) containing:
  - personal data (names, contact details)
  - reservations (airlines, hotels, cars, ...)
  - issued tickets
  - special requests
  - loyalty programs data
- Dozens of CRSs exist
  - GDS (eg. Sabre, Amadeus, Galileo, Worldspan, ...)
  - proprietary ones
- One reservation may result with multiple PNRs in different CRSs
- Data access is limited not only across CRSs, but across different parties
... and then on to other systems

- Departure Control System (DCS) – check-in info
- Advance Passenger Information (API) – to border agencies
- PNRGOV – to government agencies
- Secure Flight
| Item number | Element Description          | Field Size | Unique/Repeated | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|-------------|------------------------------|------------|----------------|----|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|
| 1           | Format Code                  | 1 U        | M             |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |
| 5           | Number of Legs Encoded       | 1 U        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |
| 11          | Passenger Name               | 20 U       | DES M AR A I S / LUC |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |
| 25 / 3      | Electronic Ticket Indicator  | 1 U        | E             |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 7           | Operating carrier PNR Code   | 7 R        | A B C 1 2 3   |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 26          | From City Airport Code       | 3 R        | Y U L         |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 38          | To City Airport Code         | 3 R        | F R A         |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 42          | Operating carrier Designator | 3 R        | A C           |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 43          | Flight Number                | 5 R        | 0 8 3 4       |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 46          | Date of Flight               | 3 R        | 2 2 8         |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 71          | Compartment Code             | 1 R        | F             |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 104         | Seat Number                  | 4 R        | 0 0 1 A       |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 107         | Check-In Sequence Number     | 5 R        | 0 0 2 5       |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 113         | Passenger Status             | 1 R        | 1             |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 6           | Field size of following variable size field | 2 R | 0 0 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 8           | Beginning of version number  | 1 U        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 9           | Version number               | 1 U        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 10          | Field size of following structured message - unique | 2 U |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 15          | Passenger Description        | 1 U        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 12          | Source of check-in           | 1 U        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 14          | Source of Boarding Pass Issuance | 1 U |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 22          | Date of Issue of Boarding Pass | 4 U |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 16          | Document Type                | 1 U        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 21          | Airline Designator of boarding pass issuer | 3 U |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 23          | Baggage Tag Licence Plate Number (s) | 13 U |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 17          | Field size of following structured message - repeated | 2 R |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 142         | Airline Numeric Code         | 3 R        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 143         | Document Form/Serial Number  | 10 R       |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 18          | Selectee indicator           | 1 R        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 108         | International Documentation Verification | 1 R |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 19          | Marketing carrier designator | 3 R        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 20          | Frequent Flyer Airline Designator | 3 R |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 236         | Frequent Flyer Number        | 16 R       |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 89          | ID/AD Indicator              | 1 R        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 118         | Free Baggage Allowance       | 3 R        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 4           | For individual airline use   | Var R      |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 25          | Beginning of Security Data   | 1 U        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 28          | Type of Security Data        | 1 U        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 29          | Length of Security Data      | 2 U        |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
| 30          | Security Data                | Var U      |               |    |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |

Source: IATA
Title: MR  First Name: JOHN  Last Name: BRAVO
PNR: QR5172
From: LHR  To: JFK  Flight No: AA51
Date (YYYY-MM-DD): 2016-04-08
Class: Business  Seat: 12A  Seq No: 15

M1BRAVO/JOHNMR  EQR5172 LHRJFKAA 0051 099C012A0015 100
Paper is just a bit less fun...

• MS Word is a great PDF-editing tool 😊
• Most likely barcode will be scanned anyway, so it needs to reflect the printed information
Lounge access

• Contract lounges
  • no way to verify eligibility
  • may require an invitation issued from the airline at check-in

• Airline-operated lounges
  • may have access to passenger records ...
  • ... but only for own passengers!
  • automatic gates increasingly popular (eg. SAS lounges in CPH, OSL; Turkish lounge in IST)
Show time!
Duty Free Goods

• In many countries goods are sold directly to the passenger (liquors sealed in a plastic bag)
• Eligibility is determined based on destination (eg. EU/Non-EU)
Where did we get?

• Free Fast Track for all
• Free lunch and booze for all
• Duty free shopping for all
Digital Signature

• In 2008 IATA extended BCBP standard with support for digital signatures based on PKI

• The field is "optional and to be used only when required by the local security administration"

• The field has variable length, with specific algorithm etc. determined by the authority

• Private keys owned by airlines, public keys distributed to third parties

• TSA enforced for US carriers
BCBP XML

• In 2008 IATA proposed Passenger and Airport Data Interchange Standards (PADIS) XML to be used for exchange of BCBP data between airlines and third parties, such as lounges or security checkpoints

• The terminal would send a message consisting of a header and full BCBP content

• The airline would reply with a Yes/No, along with a reason and optional free text
Secure Flight

• Program implemented by TSA in 2009 to match passenger data against watch lists such as No Fly List and Selectee List

• In 2013 TSA started networking CAT/BPSS devices to pull passenger data from Secure Flight, including:
  • Passenger’s full name
  • Gender
  • Date of birth
  • Screening status
  • Reservation number
  • Flight itinerary (in order to determine which airports receive data)
Is it a vulnerability?

• LOT Polish Airlines:
  - Please contact Warsaw Airport about this issue as they’re responsible for boarding pass scanning systems.

• Warsaw Airport:
  - It’s a known issue, but not a problem. We’re compliant with all CAA guidelines.

• Civil Aviation Authority for Poland:
  - Boarding pass forgery is a crime since they are documents.

• Me:
  - Can you have a legally binding document without any form of authentication?

• Civil Aviation Authority for Poland:
  - Oh, go f*** yourself!
Is it a vulnerability?

• Turkish Airlines:
  - *Please be inform that, we have already shared your contact details with our related unit, to get in touch with you as soon as possible.*

• SAS:
  - *We appreciate that you have taken the time to send us your feedback, as this is crucial for us to improve our services.*

• TSA:
  awkward silence
Will it fly?

• NO.
• Seriously. Don’t try!
But you can have a nice souvenir 😊
Sources/Further reading

- IATA: BCBP Implementation Guide

- IATA: Bar-Coded Boarding Passes FAQ

- IATA: Passenger and Airport Data Interchange Standards (PADIS) Board
  http://www.iata.org/whatwedo/workgroups/Pages/padis.aspx

- TSA: Privacy Impact Assessment for the Boarding Pass Scanning System
  https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_bpss.pdf

- TSA: Secure Flight

- BCBP Working Group: Business Requirements: BCBP Data Exchange
  http://www.aci.aero/media/aci/file/aci_priorities/it/doc0803_br3_bcbp_xmlfinal.pdf

- Bruce Schneier: Flying On Someone Else's Airplane Ticket

- Bruce Schneier: The Boarding Pass Brouhaha

- Andy Bowers: A Dangerous Loophole in Airport Security
  http://www.slate.com/articles/news_and_politics/hey_wait_a_minute/2005/02/a_dangerous_loophole_in_airport_security.html

- Christopher Sokhoian: Insecure Flight: Broken Boarding Passes and Ineffective Terrorist Watch Lists

- Jeffrey Goldberg: The Things He Carried (The Atlantic)

- Charles C. Mann: Smoke Screening (Vanity Fair)
  http://www.vanityfair.com/culture/2011/12/tsa-insanity-201112

  http://krebsonsecurity.com/2015/10/whats-in-a-boarding-pass-barcode-a-lot/