Where in the World Is Carmen Sandiego?

Karsten Nohl <nohl@srlabs.de>
Nemanja Nikodijević <nemanja@srlabs.de>
Global booking systems store data from airlines and passengers

Booking agents

- Booking web sites
- Travel agencies

Booking systems / GDS

- Fares
- Availability
- Reservations

Travel providers

- Airlines
- Hotels
- Car rental companies

Create reservations

Update fares, Change availability rules
Fare

TAP (TP) OLDEUSTP HAM to SFO

General notes
BASIC SEASON ECONOMY ONE WAY SPECIAL EXCURSION FARES
Between EUROPE and THE UNITED STATES APPLIES FOR ONE WAY FARES

Category 3: Seasonal restrictions
PERMITTED 01NOV THROUGH 15DEC OR 31DEC THROUGH 12MAY FOR EACH TRIP.

Category 4: Flight restrictions
IF THE FARE COMPONENT INCLUDES TRAVEL WITHIN EUROPE
THEN THAT TRAVEL MUST BE ON ONE OR MORE OF THE FOLLOWING ANY TP FLIGHT OPERATED BY TP ...

Availability

<table>
<thead>
<tr>
<th>Flight</th>
<th>Stops</th>
<th>Depart</th>
<th>Arrive</th>
<th>Aircraft</th>
<th>Frequency Reliability</th>
<th>Available Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP 567</td>
<td>0</td>
<td>HAM 12/31/16 6:00 AM</td>
<td>LIS 12/31/16 8:30 AM</td>
<td>319</td>
<td>Sa 87% / 13m</td>
<td>C4 D4 ZL JC PC RL Y9 B9 M9 S3 HL QL VL WL AC KC LC UC EC TC OC GR NL</td>
</tr>
<tr>
<td>TP 201</td>
<td>0</td>
<td>LIS 12/31/16 11:20 AM</td>
<td>EWR 12/31/16 2:50 PM</td>
<td>332</td>
<td>M,W,F,Sa 73% / 21m</td>
<td>C4 D4 ZL JC PC RL Y9 B9 M9 S3 HL QL VL WC AC KC LC UC EC TC OC GR NL</td>
</tr>
<tr>
<td>TP (UA) 8490</td>
<td>0</td>
<td>EWR 12/31/16 5:05 PM</td>
<td>SFO 12/31/16 8:25 PM</td>
<td>757</td>
<td>Su,Sa 72% / 32m</td>
<td>C4 D4 Z4 J4 YC BC MC SC HC QC VC WC AC KC LC UC EC TC</td>
</tr>
</tbody>
</table>
GDS also store reservations including personal information.

**ELECTRONIC TICKET**

**F 1.1HASBROUCK/EDWARDM**

**WW1ACWW 29AUG PNMES5**

1. AC 761 A SA 9SEP YULSF0 HK1 0830 1130 CANY

**FONE-**

1. **WW1-A** 1415 824-8562
2. **WW1-P** 1 415 824-0214
3. **WW1-A** 1130 TREAT AVE./**SAN FRANCISCO CA/94110 US
4. **WW1-A** AINCANAF//HASBROUCK.ORG/MEMBER EMAIL

**TKT-**

1. 1 K29AUGWW1WW 0142138066453

**AP FAX-**

1. 1 SSRFOTVYYP1 /UA00168716753

**RMKS-**

1. **C/H IS EDWARD HASBROUCK/CA USER ENTERED CREDIT CARD/USD 248**
2. **.78/ALL PSGWEB BOOKING/EMAIL TO C/H**
3. **MOP: CHARGE MY CREDIT CARD**
4. **PASSENGER REQUESTED I/R DELIVERY BY EMAIL TO AIRCANADA//HASBROUCK.ORG**
5. **TIDGERGJK1J4**

**BKIP 172.24.96.31 29AUG06 17:22**

---HISTORY---

RCVD-INTERNET PNR GUEST

**WW1 AC WW 1723Z/29AUG**

**WW1 GS WW 10IBM01 1723Z/29AUG**

NO FLOWN SEGS
Three GDS dominate the market

Booking agents

GDS

Airlines (examples)

Expedia

Amadeus

Sabre

Galileo (now part of Travelport)

Lufthansa

AirBerlin

American Airlines

Aeroflot

Example: An American Airlines ticket booked through Expedia is kept in Amadeus and Sabre

Not really used by airlines
We were curious about the protection of passenger information

<table>
<thead>
<tr>
<th>Our research motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GDS may be insecure:</strong></td>
</tr>
<tr>
<td>▪ Booking systems (GDS) go back to the 70s and 80s</td>
</tr>
<tr>
<td>▪ They were the first “cloud” before the term (or the Internet) existed</td>
</tr>
<tr>
<td>▪ Can such systems have modern security?</td>
</tr>
<tr>
<td><strong>GDS may be secure:</strong></td>
</tr>
<tr>
<td>▪ Passenger data has been in dispute between governments for years</td>
</tr>
<tr>
<td>▪ Especially the EU expressed strong political will to protect traveler data</td>
</tr>
</tbody>
</table>

Which **web service security basics** are implemented in GDS?

- Fine-grained access control  ?
- Strong authentication  ?
- Rate-limiting  ?
- Logging  ?
GDS have very coarse access restrictions

Access control: Very little

- Booking agents can access any ticket connected to the agency
- GDS staff can access all PNRs
- One PNR (can include different airlines)
- Airline staff can access all PNRs that are in any way connected to that airline

Too much access – plenty of people have access to private booking details:
1. Employees of the travel agency/website that created the booking
2. Employees of the travel providers included on the PNR
3. Employees of any of the GDS involved in any part of the PNR, including external support companies
4. Allegedly the US DHS

Too much information –
- The PNR includes all info from different providers (flight, hotel, car) for providers to see
- Includes payment information address, credit card incl. expiry
Are booking systems protected with basic security controls?

**Web service security basics**

- Fine-grained access control
- Strong authentication
- Rate-limiting
- Logging

Security Research Labs
Authentication options range from weak to very weak

**Authentication: Fail**

- Traditionally over direct connections
- Today as web service that connects over the open Internet
- Passwords often terrible

**Travel/airline agent access**
- Forgot to assign user names or passwords, oops!
- Let’s use last name as user name; and booking code / PNR locator as password
- These “passwords” cannot be changed and are widely shared between operators

**Traveler access**
- User: <Agent id>
- pw: WS<DDMMYY>
- GDS
- Login: <Last name>
- <Booking code>
- Traveler

Traditionally over direct connections
Today as web service that connects over the open Internet
Passwords often terrible

Forgot to assign user names or passwords, oops!
Let’s use last name as user name; and booking code / PNR locator as password
These “passwords” cannot be changed and are widely shared between operators
PNRs can be gathered offline
PNRs can be gathered online
Are booking systems protected with basic security controls?

**Web service security basics**

- Fine-grained access control
- Strong authentication
- Rate-limiting
- Logging
Travelers’ private information is accessible

**PNR abuse**

Anybody with access to the PNR locator (6-digit number) and last name can access:
- Identity details; possibly including hotels and car rentals
- Frequent flyer details
- Contact information: Phone number, e-mail address, often postal address
- Often date of birth and passport details

Agents (or hackers) with direct GDS access also see:
- Payment information: Credit card # and expiry
- IP address (if booked online)

**Abuse Scenarios**

<table>
<thead>
<tr>
<th><strong>Stalking</strong></th>
<th>Photo of luggage tag or boarding pass</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tracking</strong></td>
<td>Last name</td>
</tr>
<tr>
<td></td>
<td>PNR brute force search</td>
</tr>
</tbody>
</table>

Travel details, contact info
Fraudsters can possibly steal flights

**PNR abuse**

- Airlines typically only authenticate passengers with the PNR locator, even for ticket changes
- Different airlines allow different actions:
  - All allow date and flight changes (at least on some tickets)
  - Few allow name changes
  - Most allow some form of refund, often for a coupon

**Abuse Scenarios**

1. Bruteforce search tickets for common name
2. Select flexible ticket
3. Change name, e-mail, and date
4. Refund for credit in PNR
5. Refund for MCO*
6. Book new flight with credit
7. Change e-mail and date and take the flight (on an airline that does not check ID)
8. Fly for free

* Miscellaneous charges order
Miles can be stolen, fully remotely

- Adding a miles number (with the right name) to a booking diverts a victim’s miles
- Miles can be redeemed for free flights, hotel nights, or gift certificates

Abuse Scenario

1. Bruteforce search for common name
2. Selects expensive tickets
3. Create miles account in passenger name
4. Add or change miles account in booking
5. Convert on redeem collected miles

Example

- EU-Australia Round-trip 10,000 miles
- First class \(\times 3\) 60,000 miles
- \(~ 900 USD\)
All path to a booking need to be secured

American Airlines asks for first name

Find a reservation

( * Required)
Passenger first name *
| 
Passenger last name *

Record locator *

Find reservation

ViewTrip + TripCase provide alternative path w/o first name

1. Brute-force PNR + last name on ViewTrip

2. Check details on TripCase
# PNRs can be guessed

**Guessability**

<table>
<thead>
<tr>
<th>Entropy</th>
<th>Sequential</th>
<th>Amadeus</th>
<th>Sabre</th>
<th>Galileo</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.6 bits:</td>
<td>✓</td>
<td>1&lt;sup&gt;st&lt;/sup&gt; digit: 2-8, X-Z</td>
<td>✓</td>
<td>1&lt;sup&gt;st&lt;/sup&gt;-6&lt;sup&gt;th&lt;/sup&gt;: 2-9, A-Z</td>
</tr>
<tr>
<td>2&lt;sup&gt;nd&lt;/sup&gt;-6&lt;sup&gt;th&lt;/sup&gt;: 2-9, A-Z</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28.2 bits:</td>
<td>❌</td>
<td>1&lt;sup&gt;st&lt;/sup&gt;-6&lt;sup&gt;th&lt;/sup&gt;: A-Z</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Namespace split by airline)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28.9 bits:</td>
<td>✓</td>
<td>1&lt;sup&gt;st&lt;/sup&gt;: 1-9, A-Z (except F-I, O, U, Y)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2&lt;sup&gt;nd&lt;/sup&gt;-5&lt;sup&gt;th&lt;/sup&gt;: 0-9, B-Z (except E, I, O, U, Y)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6&lt;sup&gt;th&lt;/sup&gt;: 0-9, A-Z, but last bit ignored!</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Brute-force susceptibility**

<table>
<thead>
<tr>
<th>GDS-provided</th>
<th>Airlines (examples)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CheckMyTrip</td>
<td>Lufthansa</td>
</tr>
<tr>
<td>Classic: ✓ → killed</td>
<td>✓</td>
</tr>
<tr>
<td>Current: ✓ → ineffective Captcha, max 1,000 requests/IP</td>
<td></td>
</tr>
<tr>
<td>Virtually There</td>
<td>Air Berlin</td>
</tr>
<tr>
<td>Direct PNR access for some airlines (e.g. Etihad), for others: redirect to airline website (e.g. AA, Aeroflot)</td>
<td>max 1,000 rqs ⇒ Captcha</td>
</tr>
<tr>
<td>View Trip</td>
<td>American Airlines</td>
</tr>
<tr>
<td>✓</td>
<td>✓ + First name</td>
</tr>
<tr>
<td></td>
<td>Aeroflot</td>
</tr>
<tr>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Not really used by airlines, but instead by booking agents</td>
<td></td>
</tr>
</tbody>
</table>
Are booking systems protected with basic security controls?

Web service security basics

- Fine-grained access control
- Strong authentication
- Rate-limiting
- Logging
Data disclosure exposes travelers to targeted attacks

- Due to their sequential nature, fraudsters can find recently created PNRs
- And then send very targeted phishing e-mails

### Abuse Scenario

- **Poll for common last name and recent PNRs (in a GDS where PNRs are sequential)**
- **Fetch e-mail address from booking**
- **Phish for frequent flyer login or credit card information**

### Flight Theft

- Privacy intrusion

### Mile Diversion

- Phishing

---

From: LH.com online@booking-lufthansa.com
Subject: Booking Details | Departure: 22 August 2016 | TXL-MUC

URGENT: Please update your payment information

Lufthansa booking code: 33C3PO

Update payment

URGENT NOTICE: Your payment has been rejected
IMPORTANT: The following transaction has been rejected, so we are unable to process payment for your trip to HAMBURG DE (HAM) on 31 December. Your reservation is currently ON HOLD FOR 24 HOURS. Please update your payment information to confirm your reservation.

Passenger Information

**SANDIEGO / CARMEN MS**
Miles & More: XXXXXXXXXXX0054
Ticket no.: 220-2376788232

Receipt and additional documents
NOTE: Your receipt for this itinerary cannot currently be provided. PLEASE UPDATE YOUR PAYMENT INFORMATION.
Option for download is valid up to 90 days after end of travel.

Your itinerary

**Sat. 31 December 2016: MUNICH DE - HAMBURG DE**

<table>
<thead>
<tr>
<th>Time</th>
<th>Location</th>
<th>Terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:00 h</td>
<td>MUNICH DE MUNICH INTERNATIONAL (MUC)</td>
<td>2</td>
</tr>
<tr>
<td>08:15 h</td>
<td>HAMBURG DE (HAM)</td>
<td>2</td>
</tr>
</tbody>
</table>

Operated by: LUFTHANSA

---

If you cannot view this e-mail properly, please open the attached PDF version.
Do not reply to this e-mail.
Additional support is available via the FAQs.
Guessability issues are not limited to large GDS

**SITA**
- Only 4 digits to guess, plus one digit for airline

**Oman Air (Sabre)**
- Guess one city in itinerary instead of last name (Muscat, duh!)

**Ryan Air (Navitaire, an Amadeus subsidiary)**
- Uneven distribution makes it easier to guess PNR
- Guess 4 credit card digits instead of last name

**Pakistan International Airlines (Sabre)**
- Won the race for easiest guessability

**Other noteworthy systems we did not look at:**
- MACS (Emirates)
- Troya (Turkish Airlines)
- HP Shares (United, and others)
For years, questions were raised over who is accessing PNRs

Until today, GDS providers refuse to log read access to this private data (write access has always been logged)

Can more research motivate finally adding logging and make transparent to travelers who accesses their information?
Booking systems lack basic security controls

**Web service security basics**

- Fine-grained access control
- Strong authentication
- Rate-limiting
- Logging
We need better protected booking systems

<table>
<thead>
<tr>
<th>In summary</th>
<th>What we need</th>
</tr>
</thead>
<tbody>
<tr>
<td>A few global databases keep information on travelers, in systems that have grown for decades and now lack modern IT security</td>
<td>Limitations on which agents (and governments!) can access what information</td>
</tr>
<tr>
<td>Passengers authenticate only with their last name and a low-entropy (often sequential) booking code, which is also printed on passes and tags</td>
<td>Passwords for bookings</td>
</tr>
<tr>
<td>Numerous web interfaces permit brute-forcing of these booking codes, putting travelers’ privacy at risk</td>
<td>Minimum web service security for all exposed interfaces</td>
</tr>
<tr>
<td>Travelers will never know who accessed their information, since PNR access is intentionally not logged</td>
<td>Strict logging of any access to personal information</td>
</tr>
</tbody>
</table>

Coarse access control

Weak authentication

Insufficient rate limiting

No logging
Thank you!

Many thanks to Luca Melette, Sebastian Götte, and Patrick Lucey for making this research possible!

Thank you Ed Hasbrouck, Hendrik Scholz, and Seth Miller for very valuable feedback!

Questions?

Karsten Nohl <nohl@srlabs.de>
Nemanja Nikodijević <nemanja@srlabs.de>