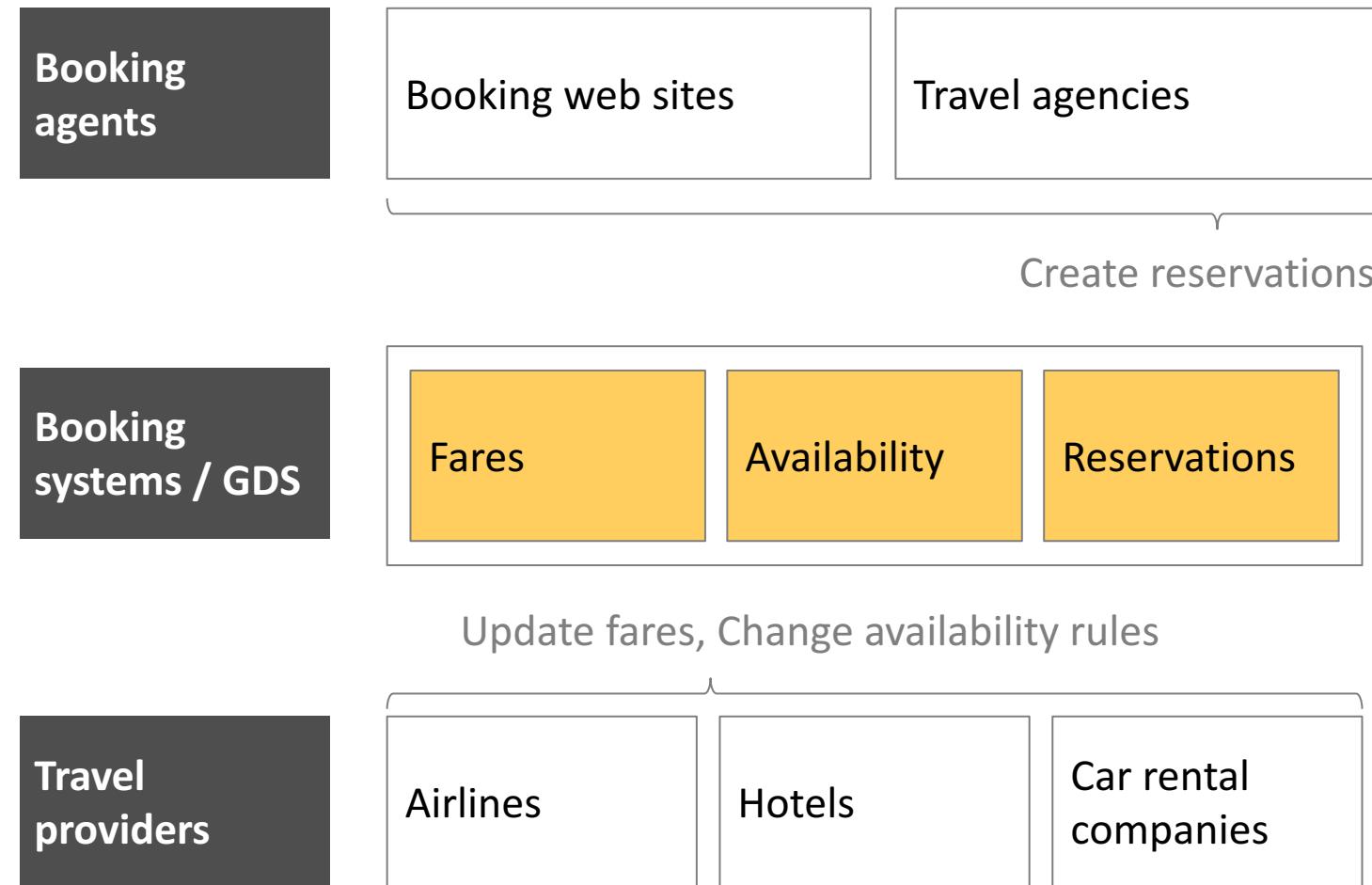


Where in the World Is Carmen Sandiego?

Karsten Nohl <nohl@srlabs.de>

Nemanja Nikodijević <nemanja@srlabs.de>

Global booking systems store data from airlines and passengers



GDS store price and availability rules

Fare



€325	Hamburg (HAM) to San Francisco (SFO) — Sat, Dec 31			
TAP	Hamburg (HAM) to Lisbon (LIS) — Sat, Dec 31	TAP 567	Dep: 6:00 am	Arr: 8:30 am
				3h 30m
			Layover in LIS	2h 50m
TAP	Lisbon (LIS) to Newark (EWR) — Sat, Dec 31			
		TAP 201	Dep: 11:20 am	Arr: 2:50 pm
				8h 30m
			Layover in EWR	2h 15m
United	Newark (EWR) to San Francisco (SFO) — Sat, Dec 31			
		United 1885	Dep: 5:05 pm	Arr: 8:25 pm
				6h 20m

Availability



Flight	Stops	Depart	Arrive	Aircraft	Frequency Reliability ?	Available Classes ? (Click on the class code for details)
2 Connections						
TP 567	0	HAM 12/31/16 6:00 AM	LIS 12/31/16 8:30 AM	319	Sa 87% / 13m	C4 D4 ZL JC PC RL Y9 B9 M9 S3 HL QL VL WL AC KC LC UC EC TC OC GR NL
TP 201	0	LIS 12/31/16 11:20 AM	EWR 12/31/16 2:50 PM	332	M,W,F,Sa 73% / 21m	C4 D4 ZL JC PC RL Y9 B9 M9 S3 HL QL VL WC AC KC LC UC EC TC OC GR NL
TP (UA) 8490	0	EWR 12/31/16 5:05 PM	SFO 12/31/16 8:25 PM	757	Su,Sa 72% / 32m	C4 D4 Z4 J4 YC BC MC SC HC QC VC WC AC KC LC UC EC TC

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 ...

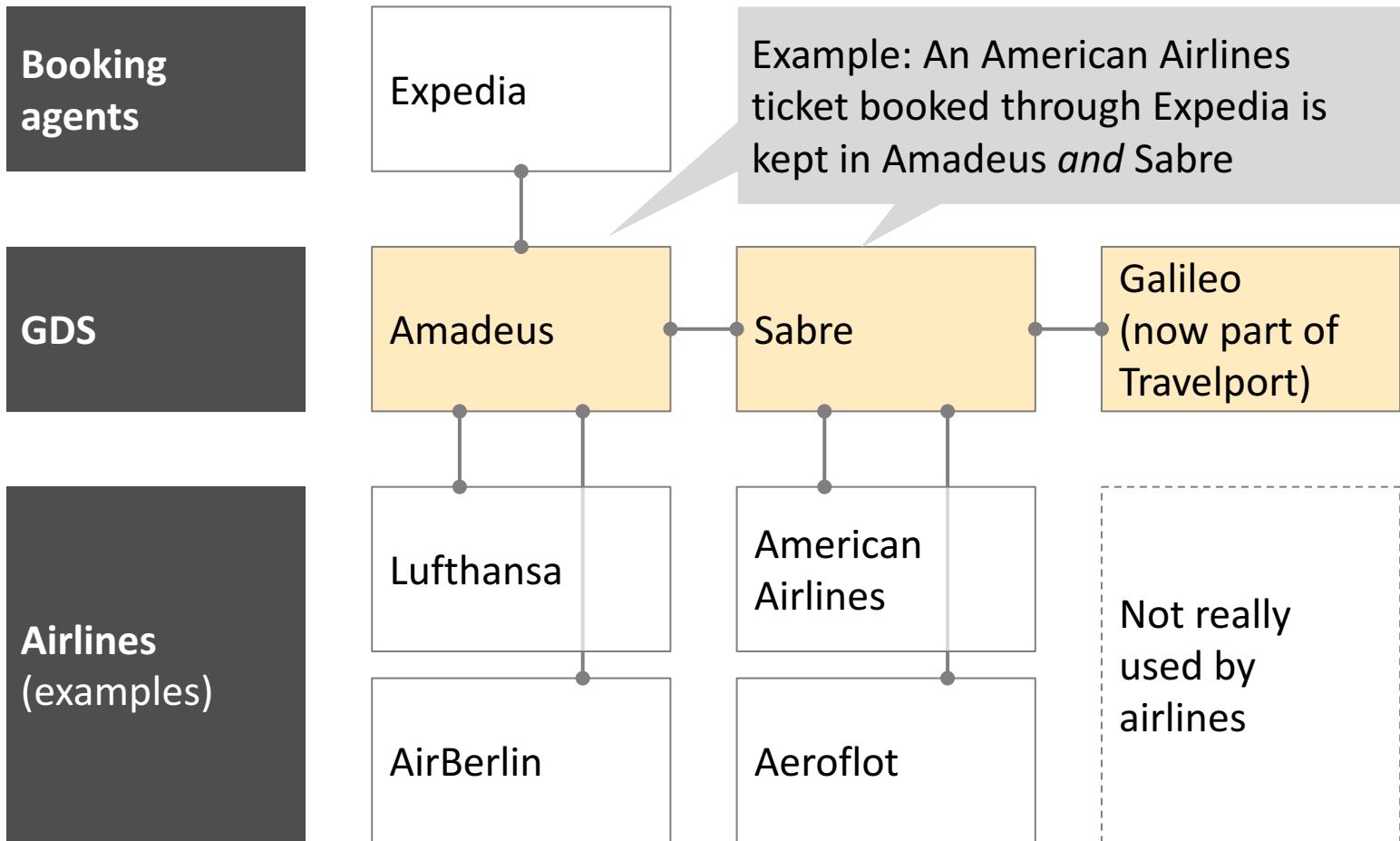
GDS also store reservations including personal information

Reservation /
PNR

62
*** ELECTRONIC TICKET ***
F 1.1HASBROUCK/EDWARDMR
WW1ACWW 29AUG PMIME5
1 AC 761 A SA 9SEP YULSFO HK1 0830 1130 CABY
FONE-
1.WW1-H 1 415 824-8562  Home and Mobile Telephone Numbers Home Address
2.WW1-P 1 415 824-0214
3.WW1-A 1130 TREAT AVE./**/SAN FRANCISCO CA/94110 US  Email Address
4.WW1-A AIRCANADA//HASBROUCK.ORG/MEMBER EMAIL 
TKT-
1.1 K29AUGWW1WW 0142138066453
AP FAX-
1.1 SSRFQTVYYPN1 /UA00168716753  Frequent Flyer Number
RMKS-
1.1 C/H IS EDWARD HASBROUCK/CA USER ENTERED CREDIT CARD/USD 248
.78/ALL PSGRWEB BOOKING/EMAIL TO C/H  Credit Card Number (redacted)
2. MOP: CHARGE MY CREDIT CARD
3. PASSENGER REQUESTED I/R DELIVERY BY EMAIL TO AIRCANADA//HASBR
OUCK.ORG
4. TIDGERGJK1J4
5. BKIP 172.24.96.31 29AUG06 17:22  Timestamped IP Address

---HISTORY---
RCVD-INTERNET PNR GUEST
WW1 AC WW 1723Z/29AUG
WW1 GS WW IOIBM01 1723Z/29AUG
NO FLOWN SEGS

Three GDS dominate the market



We were curious about the protection of passenger information

Our research motivation

GDS may be insecure:

- Booking systems (GDS) go back to the 70s and 80s
- They were the first “cloud” before the term (or the Internet) existed
- Can such systems have modern security?

GDS may be secure:

- Passenger data has been in dispute between governments for years
- Especially the EU expressed strong political will to protect traveler data

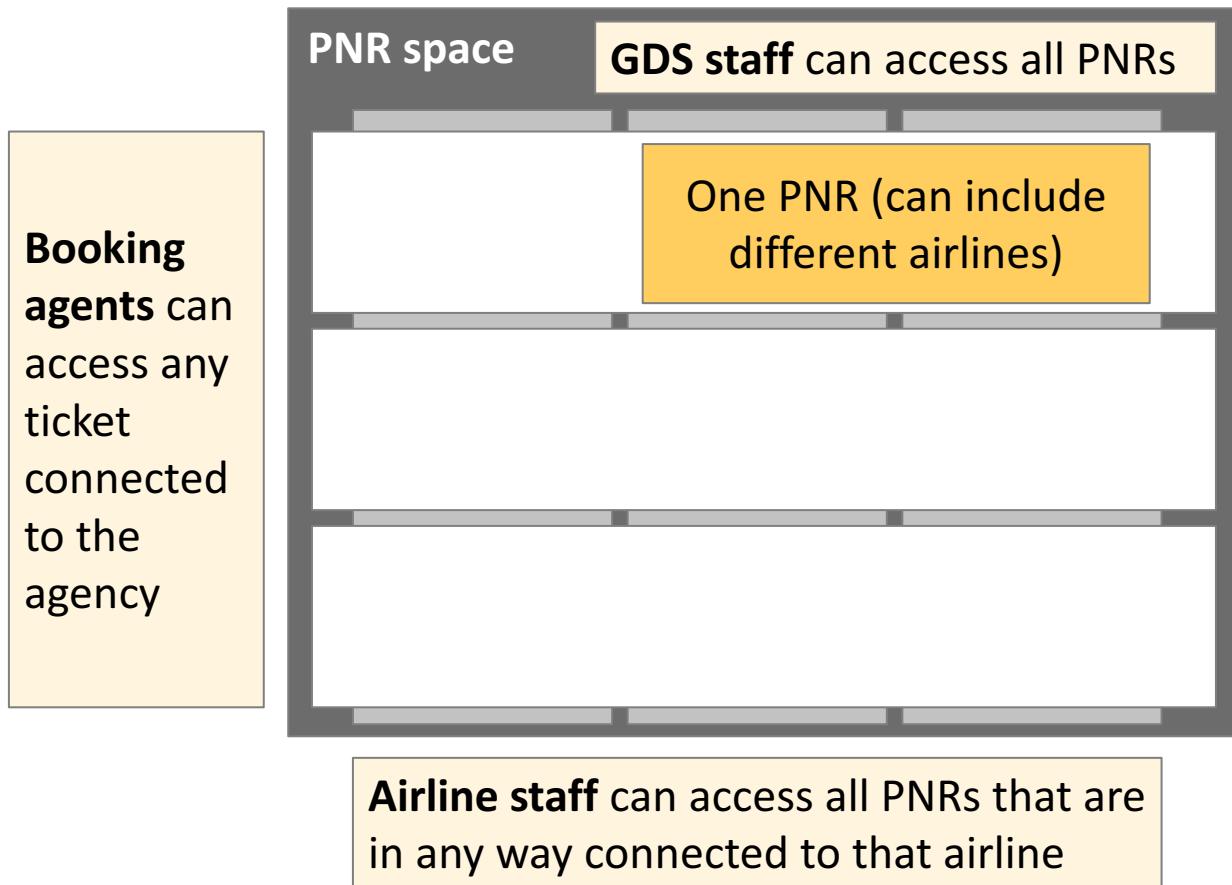
Which **web service security basics** are implemented in GDS?

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



GDS have very coarse access restrictions

Access control: **Very little**



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 

Authentication options range from weak to very weak

Authentication: Fail

Travel/airline agent access

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

Traveler 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

Agent

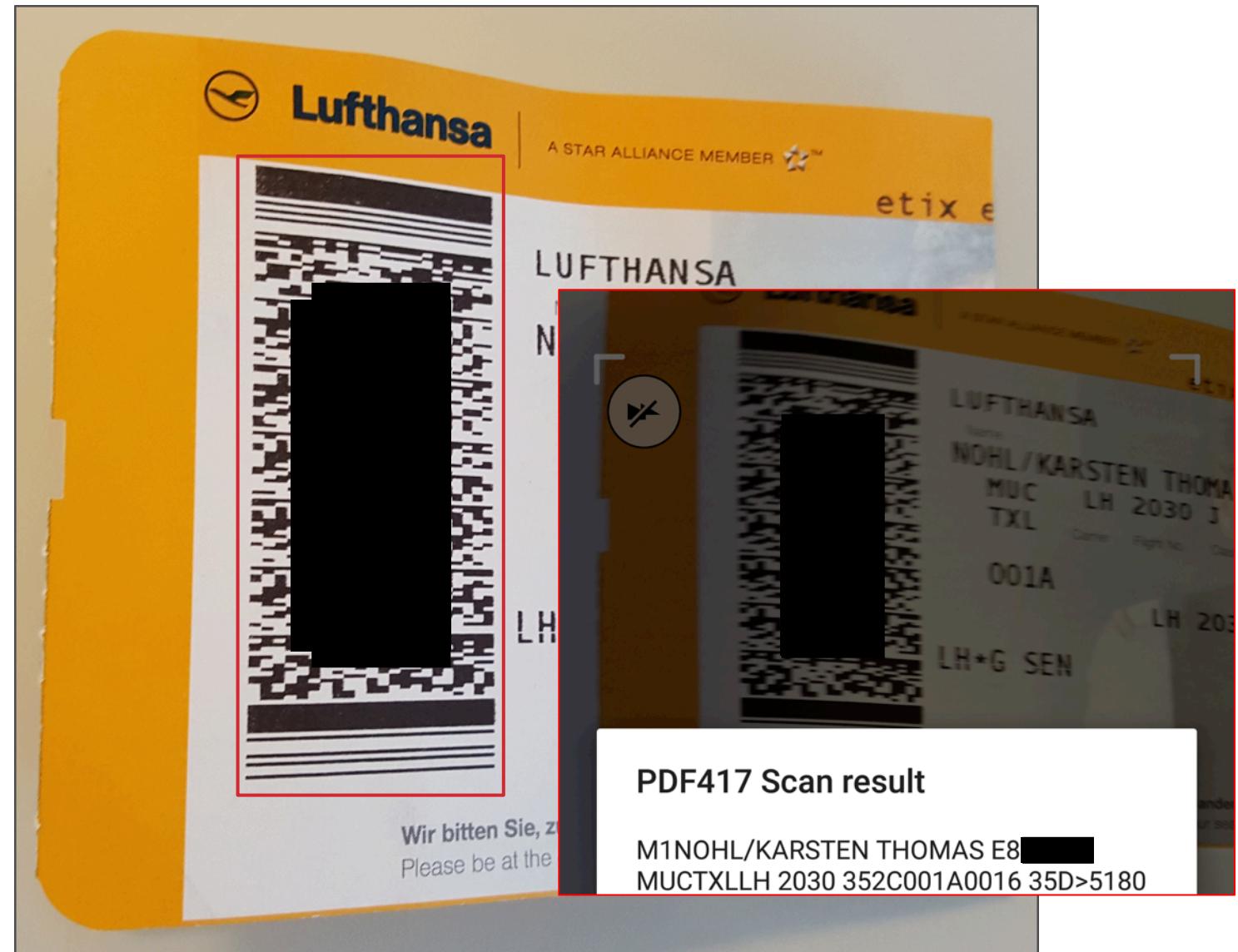
User: <Agent id>
pw: WS<DDMMYY>

GDS

Login: <Last name>
<Booking code>

Traveler

PNRs can be gathered offline



PNRs can be gathered online

Instagram



Travel details

Screenshot of the CheckMyTrip travel details page for a trip from Singapore to Brisbane on 23 Dec 2016. The page shows flight information: 1 flight, passenger JASONMR JOSEPH, and email jason@one[REDACTED]. The CheckMyTrip logo is at the top, along with a note about accepting terms and privacy policy. Navigation links for CALENDAR, PDF, and SHARE are also present.

Barcode: 1 of 1

Length: 149

Module: 1.5pix

Barcode Text processing:

Signature: IATA-BCBP

M1JOSEPH/JASON

0

B

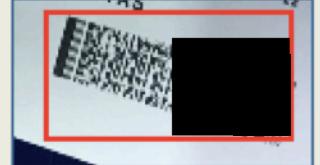
8885052

Type: Pdf417

Rotation: diagonal

Rectangle: {X=35,Y=15,Width=263,Height=136}

Page 1 of 1



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

Privacy intrusion

Flight theft

Mile diversion

Phishing

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

Stalking

Photo of luggage tag or boarding pass



Tracking

Last name

PNR bruteforce search

Travel details, contact info

Demo. PNR guessing.

Fraudsters can possibly steal flights

PNR abuse

Privacy intrusion

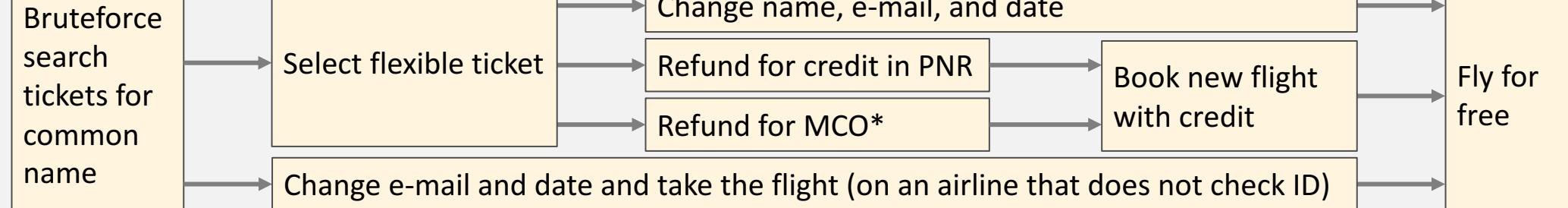
Flight theft

Mile diversion

Phishing

- 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



Miles can be stolen, fully remotely

PNR abuse

Privacy intrusion

Flight theft

Mile diversion

Phishing

- 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

Bruteforce search for common name

Selects expensive tickets

Create miles account in passenger name

Add or change miles account in booking

Convert on redeem collected miles

Miles & More



> Ab 3.000 Meilen

Example

EU-Australia	10,000 miles
Round-trip	x 2
First class	x 3
	60,000 miles
	~ 900 USD

All path to a booking need to be secured

American Airlines asks for first name

AmericanAirlines  ≡

Find a reservation

(• Required)

Passenger first name •

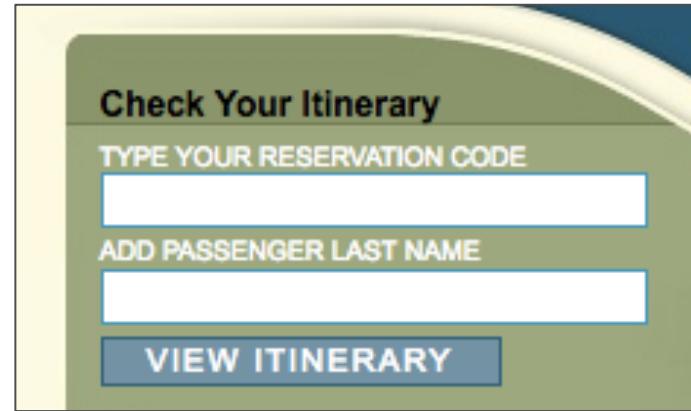
Passenger last name •

Record locator •

Find reservation

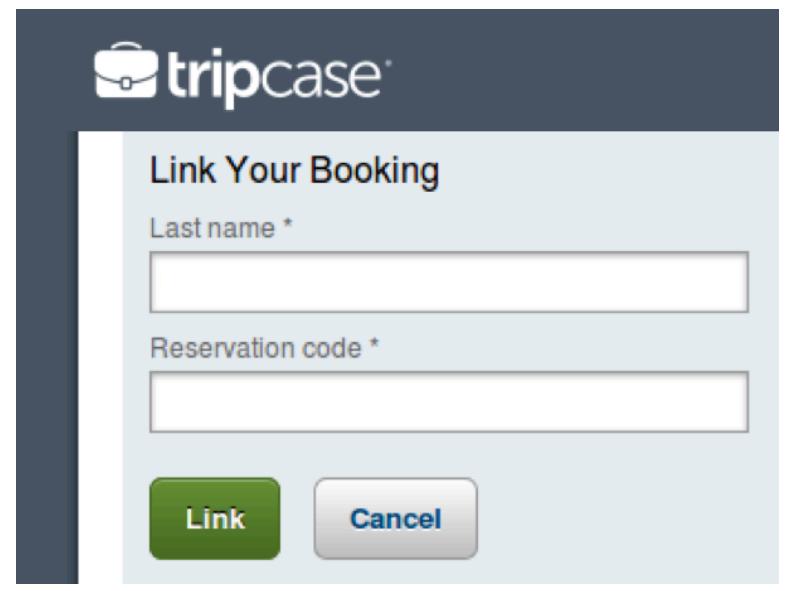
ViewTrip + TripCase provide alternative path w/o first name

1. Brute-force PNR + last name on ViewTrip



The image shows a screenshot of a web form titled "Check Your Itinerary". It has two input fields: "TYPE YOUR RESERVATION CODE" and "ADD PASSENGER LAST NAME", both with placeholder text. Below the fields is a blue button labeled "VIEW ITINERARY".

2. Check details on TripCase



The image shows a screenshot of a web form titled "Link Your Booking". It has two input fields: "Last name *" and "Reservation code *". At the bottom are two buttons: a green "Link" button and a grey "Cancel" button.

PNRs can be guessed

Guessability			
	Entropy	Sequential	Brute-force susceptibility
Amadeus	<p>28.6 bits:</p> <ul style="list-style-type: none">■ 1st digit: 2-8, X-Z■ 2nd: Depends on 1st (38 of 340 combinations invalid)■ 2nd-6th: 2-9, A-Z	✓	<p>GDS-provided</p> <p>CheckMyTrip</p> <ul style="list-style-type: none">■ Classic: ✓ → killed■ Current: ✓ → ineffective Captcha, max 1,000 requests/IP <p>Airlines (examples)</p> <p>Lufthansa</p> <ul style="list-style-type: none">■ Standard: Captcha■ Mobile: max 30 rqs/IP
Sabre	<p>28.2 bits:</p> <ul style="list-style-type: none">■ 1st-6th: A-Z■ (Namespace split by airline)	X	<p>Virtually There</p> <ul style="list-style-type: none">■ Direct PNR access for some airlines (e.g. Etihad), for others: redirect to airline website (e.g. AA, Aeroflot) <p>American Airlines</p> <p>✓ + First name</p> <p>Aeroflot</p> <p>✓</p>
Galileo	<p>28.9 bits:</p> <ul style="list-style-type: none">■ 1st: 1-9, A-Z (except F-I, O, U, Y)■ 2nd -5th: 0-9, B-Z (except E, I, O,U,Y)■ 6th: 0-9, A-Z, but last bit ignored!	✓	<p>View Trip</p> <p>✓</p> <p>Not really used by airlines, but instead by booking agents</p>

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

PNR abuse

Privacy intrusion

Flight theft

Mile diversion

Phishing

- 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

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



Lufthansa

Nonstop you

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: XXXXXXXXXXXX0054

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

07:00 h MUNICH DE MUNICH INTERNATIONAL (MUC)
TERMINAL 2

08:15 h [HAMBURG DE \(HAM\)](#)
TERMINAL 2

LH2060

operated by: LUFTHANSA

Guessability issues are not limited to large GDS

SITA

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



Ryan Air (Navitaire, an Amadeus subsidiary)

- Uneven distribution makes it easier to guess PNR
- Guess 4 credit card digits instead of last name

A screenshot of the Ryan Air booking interface. It shows fields for "Email address" and "Credit card". Below these are fields for "Reservation number" and "Credit/Debit card number", both containing placeholder text. A yellow "Go" button is at the bottom right.

Oman Air (Sabre)

A screenshot of the Oman Air booking interface titled "Manage Your Bookings". It includes fields for "Booking Reference *", "Departure Airport *", and "Time Format" (with options for 24 Hours or 12 Hours). Buttons for "View Booking" and "Exchange / Refund" are at the bottom.

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

Pakistan International Airlines (Sabre)

- Won the race for easiest guessability

A screenshot of the Pakistan International Airlines (PIA) booking interface. It features the PIA logo and Premier logo. A large green "Reservations" button is prominent. Below it is a "YOUR PNR" input field and a "Go" button.

Other noteworthy system we did not look at:

- MACS (Emirates)
- Troya (Turkish Airlines)
- HP Shares (United, and others)

PNR access is not logged

Logging/accountability: Fail



Ask Ars: Can I see what information the feds have on my travel?

One Ars editor tries to FOIA travel documents on himself.

CYRUS FARIVAR - 5/27/2014, 1:00 AM



THE PRACTICAL NOMAD

Edward Hasbrouck's blog

Wednesday, 25 August 2010

Why I'm suing the Department of Homeland Security



- 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

Coarse access control

Weak authentication

Insufficient rate limiting

No logging

In summary

- A few global databases keep information on travelers, in systems that have grown for decades and now lack modern IT security
- Passengers authenticate only with their last name and a low-entropy (often sequential) booking code, which is also printed on passes and tags
- Numerous web interfaces permit brute-forcing of these booking codes, putting travelers' privacy at risk
- Travelers will never know who accessed their information, since PNR access is intentionally not logged

What we need

- Limitations on which agents (and governments!) can access what information
- Passwords for bookings
- Minimum web service security for **all** exposed interfaces
- Strict logging of any access to personal information

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>