Travel Hacking: Hotel Edition

https://conference.hitb.org/hitbsecconf2018pek/
Beijing, China

Hendrik Scholz
hs@123.org
Agenda

- Rationale
- Data gathering
- Analytics and application
Rationale

Why am I doing this?
Isn’t a hotel room just a room?

- Room vs. suite vs. villa
- Flexible vs. non-refundable rates
- Breakfast/dinner/club lounge inclusions
- (bonus) Loyalty points
- Airport transfers, included event/theme tickets
Hotel Hacking Goals

Two distinct types of travel
Mandatory travel
Fixed travel date and destination

• Save money
• Better room
• More benefits

Memorable travel
Flexible date and destination

• Great destinations
• Awesome suites and villas
• New experiences
• Affordable

Out of scope for this presentation!
$40 Suite at Hilton Phuket, Thailand

### SUPERIOR DELUXE SUITE

138 sq. m. suite, panoramic ocean views, balcony. Executive ...

<table>
<thead>
<tr>
<th>Rate Plan</th>
<th>Price per night (THB)</th>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AARP</strong></td>
<td>¥1,235</td>
<td></td>
</tr>
<tr>
<td><strong>AAA Stay and Save</strong></td>
<td>¥1,235</td>
<td></td>
</tr>
<tr>
<td><strong>Best Available Rate</strong></td>
<td>¥1,300</td>
<td></td>
</tr>
<tr>
<td><strong>HONORS DISCOUNT</strong></td>
<td>¥1,235</td>
<td></td>
</tr>
<tr>
<td><strong>PREMIUM ROOM REWARDS</strong></td>
<td>¥1,600</td>
<td></td>
</tr>
</tbody>
</table>

**Breakfast Included**: Change or cancel up to 7 days before arrival. Includes breakfast.

**Hilton Honors Points**: 10,000

**Pay with Points & Money**:
### Intercontinental Honduras:

**Same price for all rooms**

<table>
<thead>
<tr>
<th>Room Type</th>
<th>Points Requirement</th>
<th>Price per Night</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deluxe Room</td>
<td>25,000</td>
<td>$20.00 USD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$30.00 USD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$40.00 USD</td>
</tr>
<tr>
<td>1 King Bed Suite</td>
<td>25,000</td>
<td>$20.00 USD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$30.00 USD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$40.00 USD</td>
</tr>
<tr>
<td>King Bed Presidential Suite Non-Smoking</td>
<td>25,000</td>
<td>$20.00 USD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$30.00 USD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$40.00 USD</td>
</tr>
</tbody>
</table>
$39 room including $100 Food/beverage credit at Hilton Anatole Dallas
Data Gathering
Web and app scraping
Reserve engineering APIs/Applications

• Best entry point: mobile apps
  • ~30% of hotel chains have mobile-only API
  • Standard implementation: consumption of mobile website

• Less protection on mobile APIs
  • ‘My HTTP User-Agent string is my password’

• Android better target than IOS
  • Easy APK download and static code analysis
  • Fragmented Android version landscape
    • Longer supported APIs
Reverse engineering APIs

Android app

Web browser

HTTP proxy (Burp Suite)

Hotel website
Reverse engineering details

• MITM tool
  • Burp Suite (https://portswigger.net/burp)

• Web browser
  • Set Burp as http/https proxy
  • Use User-agent plugin to pretend to be iPhone, Android, ...

• Browse website (e.g http://m.ihg.com)
  • Mimic booking process

• JSON parser: http://json.parser.online.fr/
JSON API results

- API calls recorded by Burp show results
- JSON data
- Convert results in CSV
Requirements

• Goal
  • Command line tool
  • Make tool obtain data from hotel site(s)
  • Store data in CSV format or database

• Result set
  • Property, date, room, rate, USD price, room classification

• Parameters
  • Corporate rates, promo rates, points rates
  • # of adults, stay duration
Scraper implementation

• Always assume stuff fails
  • Overloaded sites
  • Overload/scraping prevention
  • Hotels fully booked, not open yet, ...

• My implementation
  • One hotel chain per scanner (e.g. IHG, Hyatt, Hilton, ..)
  • Hotel directory scanner + per-property scanner
  • Perl WWW::Mechanize
  • Mimic Android app behavior where possible

• Parallelize everything
  • Use HTTP proxies. Assume that stuff fails!
Fail: Fixed API keys in Android apps

• Need to find origin of ‘strange’ strings in network traffic
• Bytecode from Android app (extracted using apktool)

```java
const-string v1, "x-client-id"
const-string v2, "kTZ6WF"
.line 57
invoke-interface {p1, v1, v2}, Lretrofit/RequestInterceptor$RequestFacade;
  >addHeader(Ljava/lang/String;Ljava/lang/String;)V
const-string v1, "x-client-secret"
const-string v2, "j8G44bDhxIaLNruuf3wR"
.line 58
invoke-interface {p1, v1, v2}, Lretrofit/RequestInterceptor$RequestFacade;
  >addHeader(Ljava/lang/String;Ljava/lang/String;)V
```
More Fails

• No scraping protection at all
• Hidden information in apps
  • Promotions, secret sign-up bonuses
• Left-over code on site or Android app
  • How about passing ‘X-Environment: staging’ along with request?
• Security issues
  • No certificate pinning
  • Clear text authentication
  • Site returns PIN+credit card numbers
Fun with scraping (Turning it to 11)

• There’s a radius parameter on the site
  • How about 2,000 miles?

• You can define how many hotels you want in the result set
  • How about 5,000?
  • JSON might be quite big
Implementation done right

• Congrats Marriott!
• Mobile app protected with ‘APIGuard’
  • SHA-224 HMAC for all requests

• Website uses Javascript to authenticate requests
  • Scrapable, but hard to scale
    • Requires JS engine and DOM
    • WWW::Mechanize::Chrome Perl module works
  • See commonMarriott.js requests in your browser
Using scraper data
Finding the needle in the haystack

Issues
• Lots of data
• Redundant data
• What is a good deal?

Solution: automated discovery
• Find rooms that are cheaper than usual
  • Compared to other nights
  • $ per loyalty point metrics
• Find bonuses
  • Points, free meals, SPA treatments, ...
• Find suites that are bookable
  • On points
  • For same price as regular room
Tracking prices visually

- Track price for a certain room and rate combination
- Interesting to look at but yields few results
## Currency mistakes: USD vs MXN

<table>
<thead>
<tr>
<th>Hotel Name</th>
<th>Distance</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Puebla La Noria</td>
<td>2.1 km</td>
<td>4.5</td>
</tr>
<tr>
<td>Puebla Holiday Inn Express</td>
<td>2.5 km</td>
<td>4.5</td>
</tr>
<tr>
<td>Presidente Puebla InterContinental</td>
<td>2.9 km</td>
<td>4.5</td>
</tr>
<tr>
<td>Puebla Angelopolis Holiday Inn Express</td>
<td>5.7 km</td>
<td>4.5</td>
</tr>
<tr>
<td>Puebla Crowne Plaza</td>
<td>6.2 km</td>
<td>4.5</td>
</tr>
<tr>
<td>Puebla Staybridge Suites</td>
<td>6.3 km</td>
<td>4.5</td>
</tr>
</tbody>
</table>

5 USD

1,078 MXN
1,269 MXN
84 USD
1,535 MXN
100 MXN
2,226 MXN
Price per point: Find great reward value

- Hotels sell rooms for loyalty points
  - Points value changes
  - Find sweet spots
- Compare cash rates against points rates
- Metric: CPP = US Dollar cent per point
  - Value of point in USD cent
  - Referred to as CPM (cent per mile) in air travel realm
Wyndham: Guayaquil (2019-06-29)

2 Double Beds Non-Smoking
2 Double Beds Deluxe Flat Screen Satellite TV 2 Deluxe Double Beds with pillow top, 43 inches flat screen satellite TV, air conditioning, work desk with comfort chair, coffee maker, auto-off iron and ironing board, iPhone/iPod clock radio, bathrobe, hair dryer, digital safe. Room Details

Wyndham Rewards Go Free Award
Additional Rate Details • Total for Stay
15,000 Pts

Best Available Rate
Additional Rate Details • Total for Stay
$146.67 USD/NIGHT

0.98 CPP for flexible rate, 0.73 CPP for advance purchase rate
Wyndham: Guayaquil (2019-06-29)

1 King Sleeper Sofa Suite
1 King Bed Presidential Suite nonsmoking Flat Screen Presidential Suite 3 ambiances featuring kitchen/dining room, living room and Deluxe 1 King Bed with pillow top, digital control hot tub, bathtub, shower, 43 inches flat screen satellite TV, Non-Smoking, air conditioning, work desk with comfort chair, coffee maker, auto-off iron and ironing board, iPhone/iPod clock radio, bathrobe, hair dryer, digital safe. Room Details

Wyndham Rewards Go Free Award
Additional Rate Details • Total for Stay
15,000
PTS
BOOK

Best Available Rate
Additional Rate Details • Total for Stay
$1,538
46
USD/NIGHT
BOOK

10.26 CPP for flexible rate, ~8CPP for advance purchase
Wyndham: ‘Stay twice, earn a free night’

• Promotion: Stay 2 nights, get 1 free
  • Expired, likely to come back
• Value of free night
  • $200-$1500
• Cost of two paid nights:
  • E.g. $4, $30
  • Generally <$100
Great rewards

- Intercontinental Aqaba
- All rooms
- No longer bookable

- 25k points could be purchased for ~$200. Royal Suite sells for >$1200
Newly opened hotels

• New properties lack experience
  • Typically load basic rates for all dates
  • Need to add exceptions for conferences, holidays, ...

• Look for errors
  • Suites redeemable for points
  • Suites for low cash rates
  • Cheap company/senior/AAA/... rates

• Requirement: detect new properties as quickly as possible
Delayed Opening compensation

• Book a hotel that is about to open
• Hope that it’s delayed
• Demand compensation (loyalty points) when delayed

Starwood/SPG showed opening dates on website
Best Rate Guarantees
Best Rate Guarantees (BRG, BPG)

• ‘We guarantee the best price for this room and date’
  • ... if booked on their site
• Offered by most hotel chains
  • Guarantees best price
  • Drives traffic to site (saving on commission payments)
• Compensation for valid claims
  • Price match + 20-25% rebate on rate
  • Free night
  • Gift card
IHG Best Rate Guarantee
IHG BRG: Introduction (Sept 2011)

• Started with very simple terms
• ‘If you find a cheaper rate for the same hotel + date + room + rate combination we will give you the first night free.’
• Terms must be the same
  • # of adults and children
  • Cancelation conditions
  • Inclusions (breakfast, …)
• Use meta search engines to find better rates
  • Community had known working sites for specific properties
  • Shared Google docs, …
Intended BRG Process

- Book on IHG.com
- Stumble on better rate
- Fill out BRG form
- Get BRG approved
  - Low approval rate

Optimized BRG Process

- Check rate on IHG.com
  - Use flexible rate
- Check competing sites
- Find valid claim
- Book on IHG.com
- Fill out BRG form
- Get BRG approved
  - Cancel if not
How to stay multiple nights?

Issue: Only first night free

• Use two guests
  • Day 1) guest A
  • Day 2) guest B
  • Day 3) guest A
IHG BRG: Multiple nights

• ‘Two guest attack’ busted early on
• Asked for names of all guests in room
• Compared against other claims
IHG BRG: Multiple nights Redux

- Use multiple hotels
- Day 1) hotel A
- Day 2) hotel B
- Day 3) hotel A

- Busted via ‘50 miles apart’ rule (2012)
IHG BRG: Countermeasures

• “Cannot claim hotels in your home town”
• “Reimbursement after stay rather than free stay” (2013)
• “Have to book cheapest room”
• “Only one claim per week” (2013)
IHG BRG: “flexible only” loophole

• IHG terms state
  • “You need to compare against lowest rate”
    • Usually non-refundable
  • “If no non-refundable rate is available compare against cheapest third party rate”
    • This effectively allows comparing against all IHG.com rates

• Look for almost booked out hotels
  • Easy to automate when you have data
  • Book well in advance
  • Often works when town is busy (conference, event, …)
IHG BRG: 2018 status

- No more free nights
  - Will give up to 40,000 points credit instead
  - Points based on paid rate (5x normal points)
- Flexible rate trick still works

- Still gameable
  - 40,000 points are enough for a free night
  - Consider BRG points as bonus to regular stay
  - Use points at expensive hotel
Global Distribution Networks

... or how I accidentally found the holy grail
Global Distribution Networks (GDN)

• Comparable to GDS (Amadeus, Sabre, ...) for airlines
  • Hotels (suppliers) supply inventory
  • GDN distributes data to channel partners
  • Enables room booking
• XML/SOAP interfaces
It began with a cheap room

- I was looking for a cheap room in New York
- Presidential suite had same price as regular room

- Room feature: ADA (Americans with Disabilities Act)
  - Wheelchair accessible, roll-in shower, audible/visible alarms, ...

- These rooms have their own category
  - Limited inventory, other price, ...
Look for the pillow on hyatt.com as deal indicator.
‘This looks a bit larger than usual’
Derbysoft support portal (2016)

• Found support portal by accident
  • Unprotected on the internet
  • Search key was rate code on my Hilton New York folio

• Escalated issue to Derbysoft
  • No answer. Never.
  • Fixed via Booking.com security team
Derbysoft support portal (2018)

- Revisited old support website
- Saw a familiar green website flash on my screen
- Redirected to login page

‘My adblocker can also block login windows.’
<table>
<thead>
<tr>
<th>Channel</th>
<th>Supplier Res</th>
<th>Supplier-ARI</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ameropa Pusher</td>
<td>Accor Adapter</td>
<td>DSStorage(GoPlatform UAT)</td>
<td>Config Center Manage</td>
</tr>
<tr>
<td>ATI Pusher</td>
<td>Accor Endpoint</td>
<td>DSStorage(GoPlatform UAT)</td>
<td>Config Center Manage(QA)</td>
</tr>
<tr>
<td>BestDay</td>
<td>Altura Adapter</td>
<td>DSStorage(GoPlatform CN)</td>
<td>Config Center Manage(IHG Portal)</td>
</tr>
<tr>
<td>Bookit</td>
<td>Amadeus Adapter</td>
<td>DSStorage(GoPlatform US)</td>
<td>Schedule Center</td>
</tr>
<tr>
<td>Bookit Pusher</td>
<td>AO Endpoint</td>
<td>DSStorage(TravelClick)</td>
<td>Import Changes</td>
</tr>
<tr>
<td>Doorway2</td>
<td>AO Adapter</td>
<td>DSShopStorage(GoPlatform CN)</td>
<td>ARI NoChange Report</td>
</tr>
<tr>
<td>Doorway2Demo</td>
<td>AO Adapter</td>
<td>DSShopStorage(GoPlatform US)</td>
<td>Rate-Monitor/Setting</td>
</tr>
<tr>
<td>Doorway for Despegar</td>
<td>Bestwestern Adapter(For IT)</td>
<td>DSShopStorage(Hilton Common)</td>
<td>Rate-Monitor/Report</td>
</tr>
<tr>
<td>Elong Endpoint</td>
<td>Bestwestern Adapter(For All Channel)</td>
<td>DSShopStorage(Meta Hyatt)</td>
<td>Dashboards</td>
</tr>
<tr>
<td>Elong Pusher</td>
<td>Bestwestern Adapter</td>
<td>DSStorage(UAT)</td>
<td>Availability Reporter</td>
</tr>
<tr>
<td>Expedia Automation</td>
<td>Bico Adapter</td>
<td>Shop Storage</td>
<td>IHG Portal Hotel Content</td>
</tr>
<tr>
<td>ETA</td>
<td>BookingSuite</td>
<td>DSStorage(Marriott)</td>
<td>HSE(redis)</td>
</tr>
<tr>
<td>Expedia Res Endpoint</td>
<td>Carlson Adapter</td>
<td>DSStorage(DSONE)</td>
<td>HSE(ardb)</td>
</tr>
<tr>
<td>Expedia</td>
<td>Carlson Adapter</td>
<td>DSStorage(GTA)</td>
<td>Hallway</td>
</tr>
<tr>
<td>Etstar</td>
<td>Carlson-Schedule</td>
<td>DSStorage(Micros)</td>
<td>Doorway Hotel Content</td>
</tr>
<tr>
<td>GetARoom</td>
<td>Carlson-Schedule (Standard Rate For All Channel)</td>
<td>DSStorage(Expedia Hilton)</td>
<td>DSOption Peak10</td>
</tr>
<tr>
<td>GTA</td>
<td>Carlson-Schedule</td>
<td>DSOption US</td>
<td>DSOption</td>
</tr>
<tr>
<td>GoPlatform</td>
<td>Carlson-Schedule</td>
<td>DSOption CN</td>
<td></td>
</tr>
</tbody>
</table>


Derbysoft status

• Escalated issue via suppliers.
• Somewhat fixed. Somewhat.
  • More sites found
  • Still sending clear text passwords
  • Still doing client side security
• Derbysoft never replied. replied once. Replied.
  • Slow process
  • Promised fixes
Social Engineering

They know they messed up and want to talk
Social Engineering

• Book obvious mistake (e.g. $5 room) and wait for contact
  • “Just give me the stay credit. I don’t have to stay.”
  • Allow them to save face and minimize damage

• Book more than you need
  • Book two weeks on cheap rate
  • If they cancel offer to meet in the middle and keep one

• Negotiate on (and accept) downgrades
  • Get soft benefits (breakfast, lounge access) instead of larger room

• Don’t be too persistent.
  • Accept points compensation
Mandatory travel

When you absolutely have to be at a specific place at a specific time
Saving money on mandatory travel

- Try best rate guarantees
- Use corporate codes
- Use points
- Use meta search engines
- Use cashback sites
- Look for promotions
Summary

• Lots of deals available
  • No 100% success guarantee
• Less exposure compared to air travel deals
  • Great chance of deals being honored
• Be prepared to spend lots of time with analytics/Excel/CSVs
• Hotel hunting is a fun sport
Hendrik Scholz
hs@123.org

Don’t forget to return key to front desk upon departure!