



Geo-locating Drivers: A Study of Sensitive Data Leakage in Ride-Hailing Services

Qingchuan Zhao*, Chaoshun Zuo*, Giancarlo Pellegrino^{†‡}, Zhiqiang Lin*

*The Ohio State University

†CISPA Helmholtz Center for Information Security

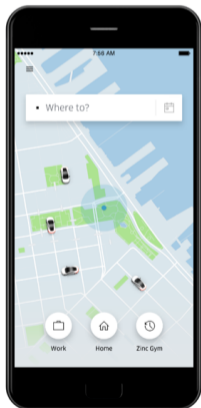
‡Stanford University

NDSS 2019

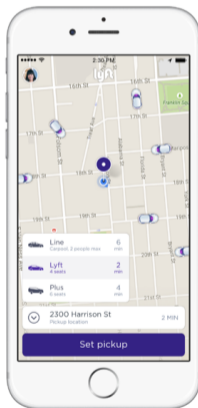


What is Ride-Hailing Service?

Uber



lyft



What is Ride-Hailing Service?



Rider App



Driver App

What is Ride-Hailing Service?



Rider App

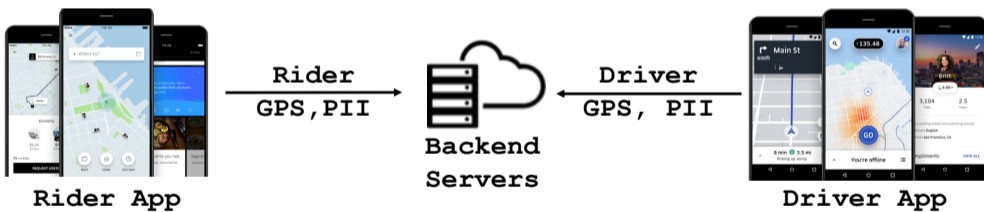


Backend
Servers



Driver App

What is Ride-Hailing Service?



Concerns with Driver's Security

Uber under assault around the world as taxi drivers fight back

Gregg Zoroya and Angela Waters, USA TODAY Published 3:44 p.m. ET July



(Photo 11: Michel Euler, AP)

Smartphone-driven Uber is revolut global backlash that includes viol New Delhi and police raids in Chi

The common anti-Uber battle cry claim Uber's business model eva

Last month, French taxi drivers ur and even taking hostages. Two U

While conceding France is a worst-case scenario, Uber says that focusing c stories.



ANGRY TAXI DRIVERS ON STRIKE ATTACK UBER TAXIS IN DOWNTOWN ATHENS (VIDEOS)

🕒 March 6, 2018 📁 Social 👁 684 Views

👍 Like 0 📌 Save 🗨 Share 1

Angry taxi drivers on work stoppage attacked Uber drivers but also their colleagues who had refused to join the 9-hour work stoppage in Athens and Attica on Tuesday. strike. It was mostly Uber drivers who

A Simplified Protocol



Rider App

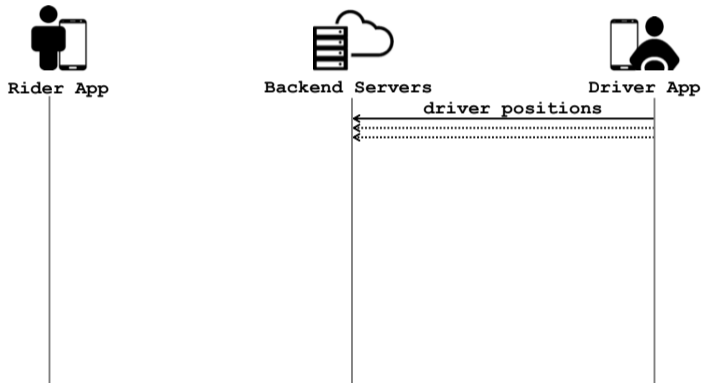


Backend Servers

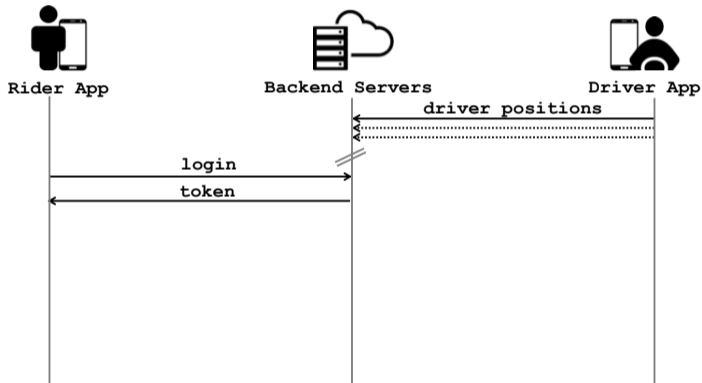


Driver App

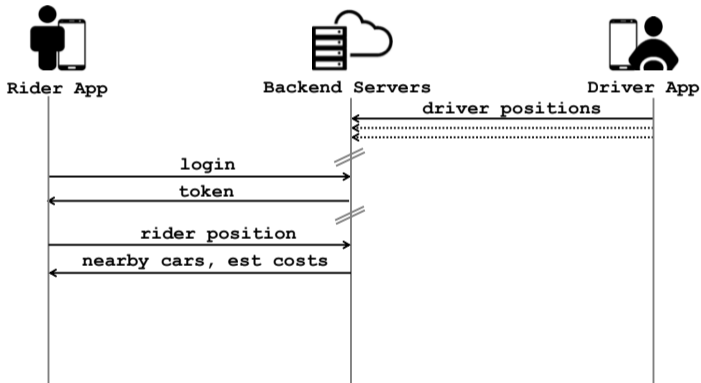
A Simplified Protocol



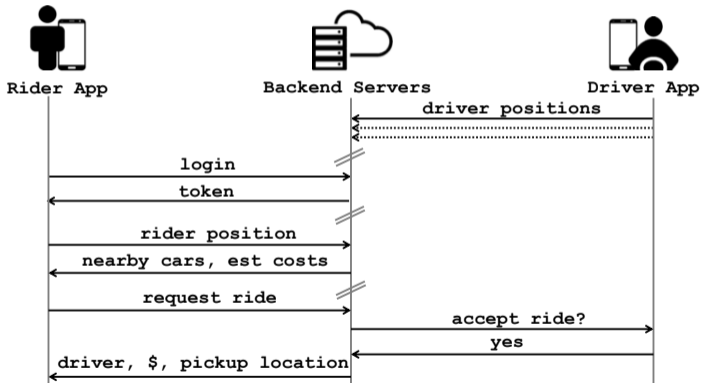
A Simplified Protocol



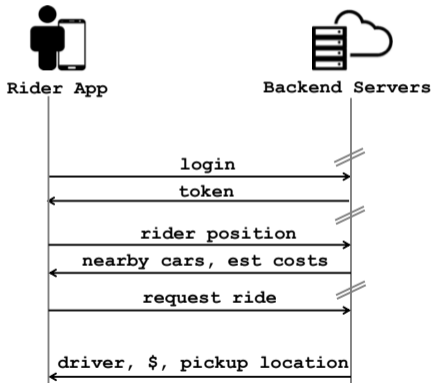
A Simplified Protocol



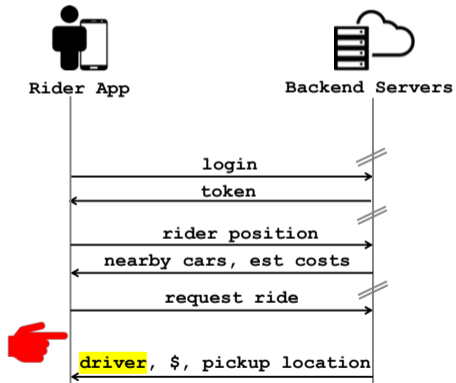
A Simplified Protocol



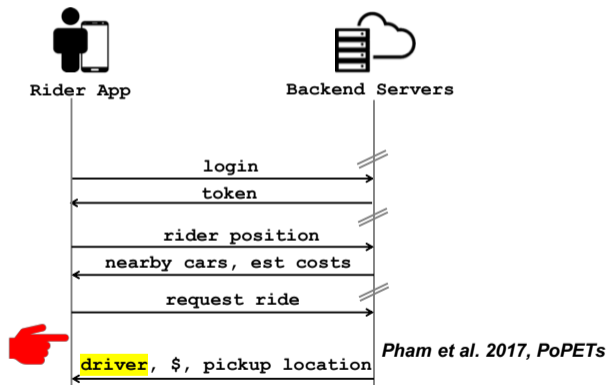
The Nearby Cars API



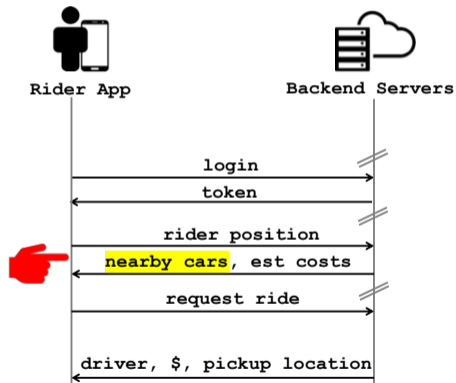
The Nearby Cars API



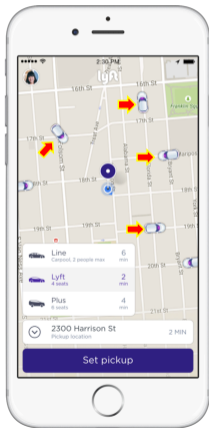
The Nearby Cars API



The Nearby Cars API



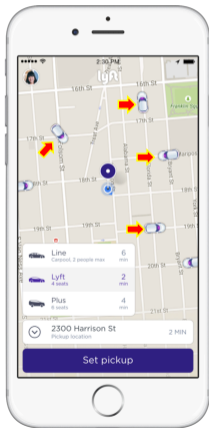
The Nearby Cars API



```
GET /nearby-cars?lat=33.7114&lng=151.1321
HTTP/1.1
...
```

```
HTTP/1.1 200 OK
Content-type: application/json
...
{
  "cars": [
    {
      "id": "509AE827",
      "positions": [
        {
          "GPS": "-33.7100 / 151.1342",
          "t": "15259620050000"
        },
        {
          "GPS": "-33.7300 / 151.1200",
          "t": "15259620060000"
        }
      ]
    },
    {
      "id": "6F09E2AA",
      ...
    },
    ...
  ]
}
```


The Nearby Cars API



The Research Questions

- 1 Private Info Leakage
 - ▶ Direct PII of Drivers
 - ▶ Movement of Drivers
 - ▶ Working Patterns of Drivers
 - ▶ Appeared Locations of Drivers
- 2 Business Info Leakage
 - ▶ Dual-Apping Driver
 - ▶ Driver Preference
 - ▶ # Drivers (Local or Global)
 - ▶ Operation Performance

App Selection

Service Name	#Downloads	APK Obfus?
Uber	100+ millions	✓
Easy	10+ millions	✓
Gett	10+ millions	✓
Lyft	10+ millions	✓
myTaxi	5+ millions	✓
Taxify	5+ millions	X
BiTaksi	1+ millions	✓
Heetch	1+ millions	✓
Jeeny	500+ thousands	✓
Flywheel	100+ thousands	X
GoCatch	100+ thousands	✓
miCab	100+ thousands	X
RideAustin	100+ thousands	X
Ztrip	100+ thousands	✓
eCab	50+ thousands	✓
GroundLink	10+ thousands	X
HelloCabs	10+ thousands	X
Ride LA	10+ thousands	X
Bounce	10+ thousands	X
DC Taxi Rider	5+ thousands	✓

App Selection

Service Name	#Downloads	APK Obfus?
Uber	100+ millions	✓
Easy	10+ millions	✓
Gett	10+ millions	✓
Lyft	10+ millions	✓
myTaxi	5+ millions	✓
Taxify	5+ millions	✗
BiTaksi	1+ millions	✓
Heetch	1+ millions	✓
Jeeny	500+ thousands	✓
Flywheel	100+ thousands	✗
GoCatch	100+ thousands	✓
miCab	100+ thousands	✗
RideAustin	100+ thousands	✗
Ztrip	100+ thousands	✓
eCab	50+ thousands	✓
GroundLink	10+ thousands	✗
HelloCabs	10+ thousands	✗
Ride LA	10+ thousands	✗
Bounce	10+ thousands	✗
DC Taxi Rider	5+ thousands	✓

App Selection

Service Name	#Downloads	APK Obfus?
Uber	100+ millions	✓
Easy	10+ millions	✓
Gett	10+ millions	✓
Lyft	10+ millions	✓
myTaxi	5+ millions	✓
Taxify	5+ millions	X
BiTaksi	1+ millions	✓
Heetch	1+ millions	✓
Jeeny	500+ thousands	✓
Flywheel	100+ thousands	X
GoCatch	100+ thousands	✓
miCab	100+ thousands	X
RideAustin	100+ thousands	X
Ztrip	100+ thousands	✓
eCab	50+ thousands	✓
GroundLink	10+ thousands	X
HelloCabs	10+ thousands	X
Ride LA	10+ thousands	X
Bounce	10+ thousands	X
DC Taxi Rider	5+ thousands	✓

App Selection

Service Name	#Downloads	APK Obfus?
Uber	100+ millions	✓
Easy	10+ millions	✓
Gett	10+ millions	✓
Lyft	10+ millions	✓
myTaxi	5+ millions	✓
Taxify	5+ millions	X
BiTaksi	1+ millions	✓
Heetch	1+ millions	✓
Jeeny	500+ thousands	✓
Flywheel	100+ thousands	X
GoCatch	100+ thousands	✓
miCab	100+ thousands	X
RideAustin	100+ thousands	X
Ztrip	100+ thousands	✓
eCab	50+ thousands	✓
GroundLink	10+ thousands	X
HelloCabs	10+ thousands	X
Ride LA	10+ thousands	X
Bounce	10+ thousands	X
DC Taxi Rider	5+ thousands	✓

A Running Example

```
GET /v1/nearby-drivers-pickup-etas?  
lat=10.10&lng=-10.10 HTTP/1.1  
Authorization: Bearer dmGtpMxlqCKeA
```

```
HTTP/1.1 200 OK  
Content-type: application/json  
{  
  "nearby_drivers": [  
    {  
      ...  
      "driver": {  
        ...  
      },  
      "locations": [  
        {  
          "lat": 10.10,  
          "lng": -10.10,  
          "recorded_at_ms": 1234  
        },  
        ...  
      ]  
    },  
    {  
      ...  
      "driver": {  
        ...  
      },  
      ...  
    }  
  ]  
}
```

(c) Nearby Cars API

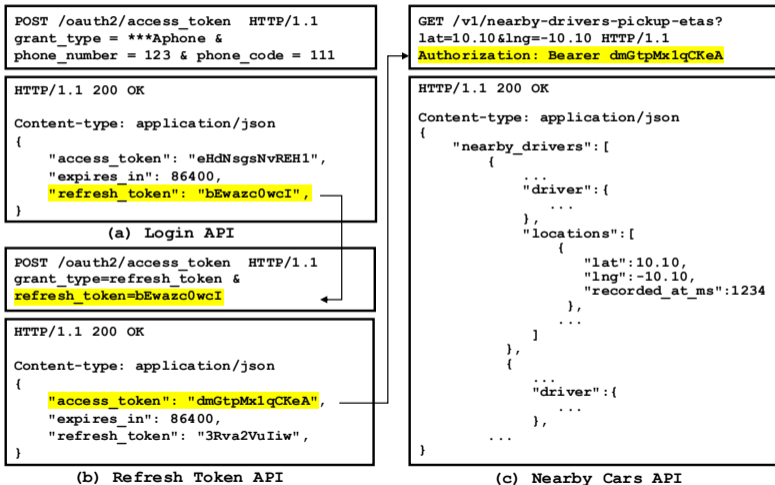
A Running Example

```
GET /v1/nearby-drivers-pickup-etas?  
lat=10.10&lng=-10.10 HTTP/1.1  
Authorization: Bearer dmGtpMxlqCKeA
```

```
HTTP/1.1 200 OK  
Content-type: application/json  
{  
  "nearby_drivers": [  
    {  
      ...  
      "driver": {  
        ...  
      },  
      "locations": [  
        {  
          "lat": 10.10,  
          "lng": -10.10,  
          "recorded_at_ms": 1234  
        },  
        ...  
      ]  
    },  
    {  
      ...  
      "driver": {  
        ...  
      },  
      ...  
    }  
  ]  
}
```

(c) Nearby Cars API

A Running Example



Automating This Process With A Tool

```
POST /oauth2/access_token HTTP/1.1
grant_type = **Aphone &
phone_number = 123 & phone_code = 111
```

HTTP/1.1 200 OK

```
Content-type: application/json
{
  "access_token": "eHdNsgsNvREH1",
  "expires_in": 86400,
  "refresh_token": "bEwazc0wci",
}
```

(a) Login API

```
POST /oauth2/access_token HTTP/1.1
grant_type=refresh token &
refresh_token=bEwazc0wci
```

HTTP/1.1 200 OK

```
Content-type: application/json
{
  "access_token": "dmGtpMxlqCKeA",
  "expires_in": 86400,
  "refresh_token": "3Rva2VuIiw",
}
```

(b) Refresh Token API

```
GET /v1/nearby-drivers-pickup-etax?
lat=10.10&lng=-10.10 HTTP/1.1
Authorization: Bearer dmGtpMxlqCKeA
```

HTTP/1.1 200 OK

```
Content-type: application/json
{
  "nearby_drivers": [
    {
      "driver": {
        ...
      },
      "locations": [
        {
          "lat": 10.10,
          "lng": -10.10,
          "recorded_at_ms": 1234
        },
        ...
      ]
    },
    ...
  ]
}
```

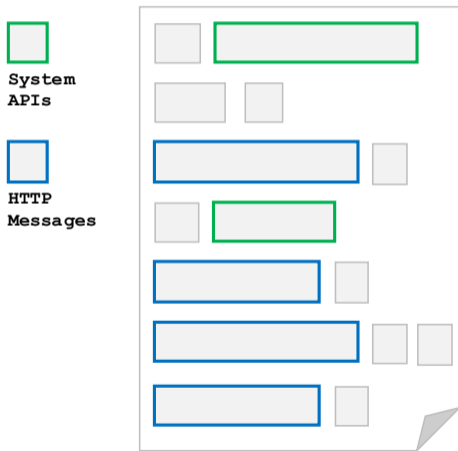
(c) Nearby Cars API

Tool Objectives

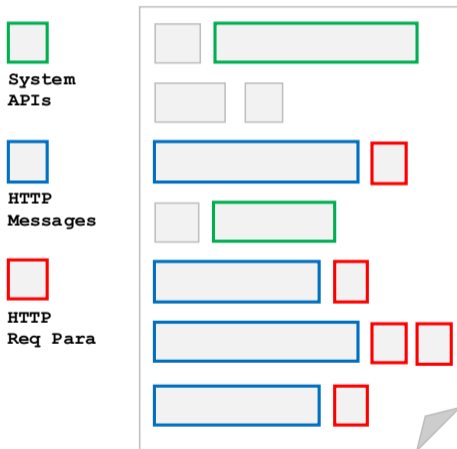
- 1 Pinpointing the Nearby Cars APIs
- 2 Identifying the Dependencies
- 3 Bypassing Obfuscations Used in the Apps

Tool Implementation: Trace the Executions of Sys/Networking APIs

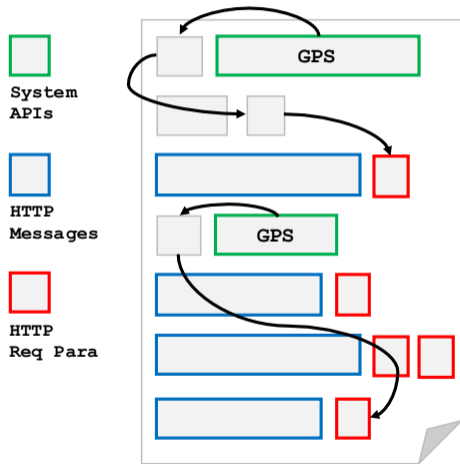
Tool Implementation: Trace the Executions of Sys/Networking APIs



Tool Implementation: Trace the Executions of Sys/Networking APIs



Tool Implementation: Trace the Executions of Sys/Networking APIs



Tool Implementation: Trace the Executions of Sys/Networking APIs

```
GET /v1/nearby-drivers-pickup-etas?  
lat=10.10&lng=-10.10 HTTP/1.1  
Authorization: Bearer dmGtpMxlqCKeA
```

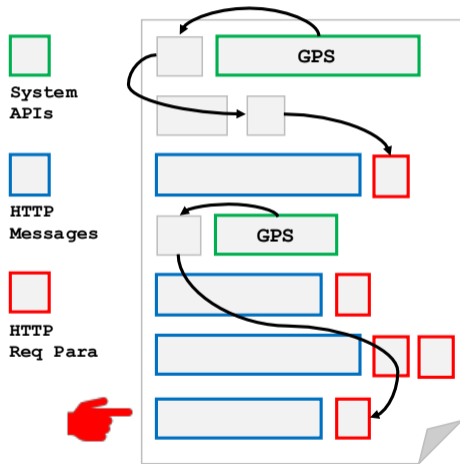
```
HTTP/1.1 200 OK  
Content-type: application/json  
{  
  "nearby_drivers": [  
    {  
      ...  
      "driver": {  
        ...  
      },  
      "locations": [  
        {  
          "lat": 10.10,  
          "lng": -10.10,  
          "recorded_at_ms": 1234  
        },  
        ...  
      ]  
    },  
    {  
      ...  
      "driver": {  
        ...  
      },  
      ...  
    }  
  ]  
}
```

Tool Implementation: Trace the Executions of Sys/Networking APIs

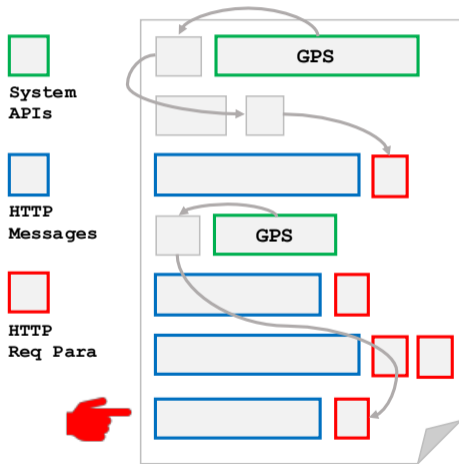
```
GET /v1/nearby-drivers-pickup-etas?  
lat=10.10&lng=-10.10 HTTP/1.1  
Authorization: Bearer dmGtpMxlqCKeA
```

```
HTTP/1.1 200 OK  
Content-type: application/json  
{  
  "nearby_drivers": [  
    {  
      ...  
      "driver": {  
        ...  
      },  
      "locations": [  
        {  
          "lat": 10.10,  
          "lng": -10.10,  
          "recorded_at_ms": 1234  
        },  
        ...  
      ]  
    },  
    {  
      ...  
      "driver": {  
        ...  
      },  
      ...  
    }  
  ]  
}
```

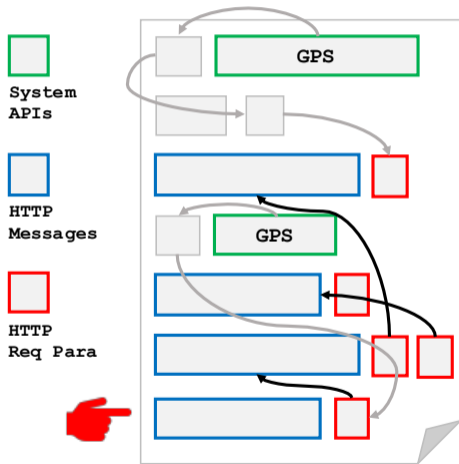
Tool Implementation: Trace the Executions of Sys/Networking APIs



Tool Implementation: Trace the Executions of Sys/Networking APIs



Tool Implementation: Trace the Executions of Sys/Networking APIs



Tool Implementation: Trace the Executions of Sys/Networking APIs

An API's Response

```
HTTP/1.1 200 OK

Content-type: application/json
{
  "access_token": "eHdNsgsNvREH1",
  "expires_in": 86400,
  "refresh_token": "bEwazc0wcI",
}
```

```
GET /v1/nearby-drivers-pickup-etas?
lat=10.10&lng=-10.10 HTTP/1.1
Authorization: Bearer dmGtpMx1qCKeA
```

Nearby Cars API's Request

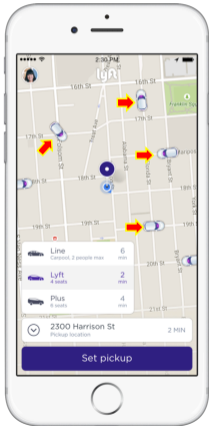
```
POST /oauth2/access_token HTTP/1.1
grant_type=refresh_token &
refresh_token=bEwazc0wcI
```

```
HTTP/1.1 200 OK

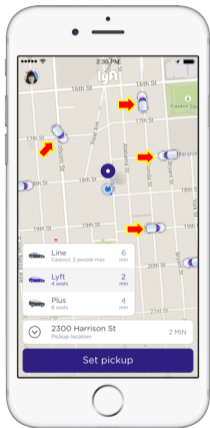
Content-type: application/json
{
  "access_token": "dmGtpMx1qCKeA",
  "expires_in": 86400,
  "refresh_token": "3Rva2VuIiw",
}
```

An API's Request and Response

Countermeasures Against Data Harvesting of The **Nearby Cars API**



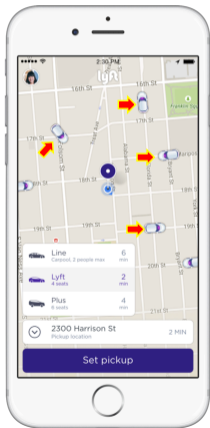
Countermeasures Against Data Harvesting of The **Nearby Cars API**



List of Countermeasures to Evaluate

- 1 Rate Limiting
 - ▶ RL1 : Reqs/s
 - ▶ RL2 : Different IPs

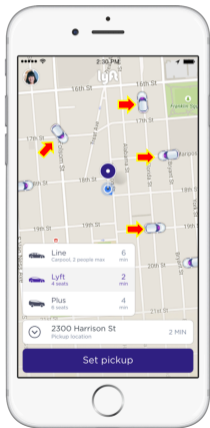
Countermeasures Against Data Harvesting of The **Nearby Cars API**



List of Countermeasures to Evaluate

- 1 Rate Limiting
 - ▶ RL1 : Reqs/s
 - ▶ RL2 : Different IPs
- 2 Session Management
 - ▶ SM1 : Authentication
 - ▶ SM2 : Session Lifespan

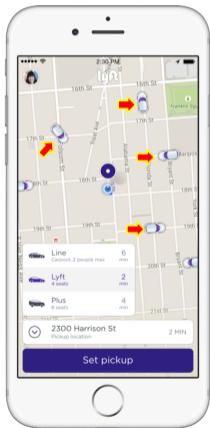
Countermeasures Against Data Harvesting of The **Nearby Cars API**



List of Countermeasures to Evaluate

- 1 Rate Limiting
 - ▶ RL1 : Reqs/s
 - ▶ RL2 : Different IPs
- 2 Session Management
 - ▶ SM1 : Authentication
 - ▶ SM2 : Session Lifespan
- 3 Anti-GPS Spoofing

Countermeasures Against Data Harvesting of The **Nearby Cars API**



List of Countermeasures to Evaluate

- 1 Rate Limiting
 - ▶ RL1 : Reqs/s
 - ▶ RL2 : Different IPs
- 2 Session Management
 - ▶ SM1 : Authentication
 - ▶ SM2 : Session Lifespan
- 3 Anti-GPS Spoofing
- 4 Anonymization
 - ▶ AN1 : Identifier Lifespan
 - ▶ AN2 : Personal Identifiable Information

Countermeasures Analysis Results

Rider App	Reqs/s	Diff IPs	Authen	Sn Lifespan	Anti-GPS	ID Lifespan	PII
Uber	●	○	●	∞	○	∞	●
Easy	-	○	○	∞	○	∞	●
Gett	-	○	●	∞	○	∞	●
Lyft	●	○	●	24h	○	∞	○
myTaxi	-	○	○	∞	○	20m	●
Taxify	●	○	●	∞	○	∞	●
BiTaksi	-	○	●	∞	○	∞	●
Heetch	-	○	●	∞	○	∞	●
Jeeny	-	○	○	∞	○	20m	●
Flywheel	-	○	●	20m	○	10m	●
GoCatch	-	○	●	∞	○	∞	●
miCab	-	○	●	∞	○	∞	○
RideAustin	-	○	●	∞	○	∞	●
Ztrip	-	○	●	30m	○	∞	●
eCab	●	○	○	∞	○	∞	●
GroundLink	-	○	○	∞	○	∞	●
HelloCabs	-	○	●	∞	○	∞	○
Ride LA	-	○	○	∞	○	∞	○
Bounce	-	○	●	∞	○	∞	○
DC Taxi Rider	-	○	●	∞	○	∞	○

Countermeasures Analysis Results

Rider App	Reqs/s	Diff IPs	Authn	Sn Lifespan	Anti-GPS	ID Lifespan	PII
Uber	●	○	●	∞	○	∞	●
Easy	-	○	○	∞	○	∞	●
Gett	-	○	●	∞	○	∞	●
Lyft	●	○	●	24h	○	∞	○
myTaxi	-	○	○	∞	○	20m	●
Taxify	●	○	●	∞	○	∞	●
BiTaksi	-	○	●	∞	○	∞	●
Heetch	-	○	●	∞	○	∞	●
Jeeny	-	○	○	∞	○	20m	●
Flywheel	-	○	●	20m	○	10m	●
GoCatch	-	○	●	∞	○	∞	●
miCab	-	○	●	∞	○	∞	○
RideAustin	-	○	●	∞	○	∞	●
Ztrip	-	○	●	30m	○	∞	●
eCab	●	○	○	∞	○	∞	●
GroundLink	-	○	○	∞	○	∞	●
HelloCabs	-	○	●	∞	○	∞	○
Ride LA	-	○	○	∞	○	∞	○
Bounce	-	○	●	∞	○	∞	○
DC Taxi Rider	-	○	●	∞	○	∞	○

Countermeasures Analysis Results

Rider App	Reqs/s	Diff IPs	Authn	Sn Lifespan	Anti-GPS	ID Lifespan	PII
Uber	●	○	●	∞	○	∞	●
Easy	-	○	○	∞	○	∞	●
Gett	-	○	●	∞	○	∞	●
Lyft	●	○	●	24h	○	∞	○
myTaxi	-	○	○	∞	○	20m	●
Taxify	●	○	●	∞	○	∞	●
BiTaksi	-	○	●	∞	○	∞	●
Heetch	-	○	●	∞	○	∞	●
Jeeny	-	○	○	∞	○	20m	●
Flywheel	-	○	●	20m	○	10m	●
GoCatch	-	○	●	∞	○	∞	●
miCab	-	○	●	∞	○	∞	○
RideAustin	-	○	●	∞	○	∞	●
Ztrip	-	○	●	30m	○	∞	●
eCab	●	○	○	∞	○	∞	●
GroundLink	-	○	○	∞	○	∞	●
HelloCabs	-	○	●	∞	○	∞	○
Ride LA	-	○	○	∞	○	∞	○
Bounce	-	○	●	∞	○	∞	○
DC Taxi Rider	-	○	●	∞	○	∞	○

Countermeasures Analysis Results

Rider App	Reqs/s	Diff IPs	Authen	Sn Lifespan	Anti-GPS	ID Lifespan	PII
Uber	●	○	●	∞	○	∞	●
Easy	-	○	○	∞	○	∞	●
Gett	-	○	●	∞	○	∞	●
Lyft	●	○	●	24h	○	∞	○
myTaxi	-	○	○	∞	○	20m	●
Taxify	●	○	●	∞	○	∞	●
BiTaksi	-	○	●	∞	○	∞	●
Heetch	-	○	●	∞	○	∞	●
Jeeny	-	○	○	∞	○	20m	●
Flywheel	-	○	●	20m	○	10m	●
GoCatch	-	○	●	∞	○	∞	●
miCab	-	○	●	∞	○	∞	○
RideAustin	-	○	●	∞	○	∞	●
Ztrip	-	○	●	30m	○	∞	●
eCab	●	○	○	∞	○	∞	●
GroundLink	-	○	○	∞	○	∞	●
HelloCabs	-	○	●	∞	○	∞	○
Ride LA	-	○	○	∞	○	∞	○
Bounce	-	○	●	∞	○	∞	○
DC Taxi Rider	-	○	●	∞	○	∞	○

Countermeasures Analysis Results

Rider App	Reqs/s	Diff IPs	Authen	Sn Lifespan	Anti-GPS	ID Lifespan	PII
Uber	●	○	●	∞	○	∞	●
Easy	-	○	○	∞	○	∞	●
Gett	-	○	●	∞	○	∞	●
Lyft	●	○	●	24h	○	∞	○
myTaxi	-	○	○	∞	○	20m	●
Taxify	●	○	●	∞	○	∞	●
BiTaksi	-	○	●	∞	○	∞	●
Heetch	-	○	●	∞	○	∞	●
Jeeny	-	○	○	∞	○	20m	●
Flywheel	-	○	●	20m	○	10m	●
GoCatch	-	○	●	∞	○	∞	●
miCab	-	○	●	∞	○	∞	○
RideAustin	-	○	●	∞	○	∞	●
Ztrip	-	○	●	30m	○	∞	●
eCab	●	○	○	∞	○	∞	●
GroundLink	-	○	○	∞	○	∞	●
HelloCabs	-	○	●	∞	○	∞	○
Ride LA	-	○	○	∞	○	∞	○
Bounce	-	○	●	∞	○	∞	○
DC Taxi Rider	-	○	●	∞	○	∞	○

Countermeasures Analysis Results

Rider App	Reqs/s	Diff IPs	Authen	Sn Lifespan	Anti-GPS	ID Lifespan	PII
Uber	●	○	●	∞	○	∞	●
Easy	-	○	○	∞	○	∞	●
Gett	-	○	●	∞	○	∞	●
Lyft	●	○	●	24h	○	∞	○
myTaxi	-	○	○	∞	○	20m	●
Taxify	●	○	●	∞	○	∞	●
BiTaksi	-	○	●	∞	○	∞	●
Heetch	-	○	●	∞	○	∞	●
Jeeny	-	○	○	∞	○	20m	●
Flywheel	-	○	●	20m	○	10m	●
GoCatch	-	○	●	∞	○	∞	●
miCab	-	○	●	∞	○	∞	○
RideAustin	-	○	●	∞	○	∞	●
Ztrip	-	○	●	30m	○	∞	●
eCab	●	○	○	∞	○	∞	●
GroundLink	-	○	○	∞	○	∞	●
HelloCabs	-	○	●	∞	○	∞	○
Ride LA	-	○	○	∞	○	∞	○
Bounce	-	○	●	∞	○	∞	○
DC Taxi Rider	-	○	●	∞	○	∞	○

Countermeasures Analysis Results

Rider App	Reqs/s	Diff IPs	Authen	Sn Lifespan	Anti-GPS	ID Lifespan	PII
Uber	●	○	●	∞	○	∞	●
Easy	-	○	○	∞	○	∞	●
Gett	-	○	●	∞	○	∞	●
Lyft	●	○	●	24h	○	∞	○
myTaxi	-	○	○	∞	○	20m	●
Taxify	●	○	●	∞	○	∞	●
BiTaksi	-	○	●	∞	○	∞	●
Heetch	-	○	●	∞	○	∞	●
Jeeny	-	○	○	∞	○	20m	●
Flywheel	-	○	●	20m	○	10m	●
GoCatch	-	○	●	∞	○	∞	●
miCab	-	○	●	∞	○	∞	○
RideAustin	-	○	●	∞	○	∞	●
Ztrip	-	○	●	30m	○	∞	●
eCab	●	○	○	∞	○	∞	●
GroundLink	-	○	○	∞	○	∞	●
HelloCabs	-	○	●	∞	○	∞	○
Ride LA	-	○	○	∞	○	∞	○
Bounce	-	○	●	∞	○	∞	○
DC Taxi Rider	-	○	●	∞	○	∞	○

Countermeasures Analysis Results

Rider App	Reqs/s	Diff IPs	Authen	Sn Lifespan	Anti-GPS	ID Lifespan	PII
Uber	●	○	●	∞	○	∞	●
Easy	-	○	○	∞	○	∞	●
Gett	-	○	●	∞	○	∞	●
Lyft	●	○	●	24h	○	∞	○
myTaxi	-	○	○	∞	○	20m	●
Taxify	●	○	●	∞	○	∞	●
BiTaksi	-	○	●	∞	○	∞	●
Heetch	-	○	●	∞	○	∞	●
Jeeny	-	○	○	∞	○	20m	●
Flywheel	-	○	●	20m	○	10m	●
GoCatch	-	○	●	∞	○	∞	●
miCab	-	○	●	∞	○	∞	○
RideAustin	-	○	●	∞	○	∞	●
Ztrip	-	○	●	30m	○	∞	●
eCab	●	○	○	∞	○	∞	●
GroundLink	-	○	○	∞	○	∞	●
HelloCabs	-	○	●	∞	○	∞	○
Ride LA	-	○	○	∞	○	∞	○
Bounce	-	○	●	∞	○	∞	○
DC Taxi Rider	-	○	●	∞	○	∞	○

Countermeasures Analysis Results

Rider App	Reqs/s	Diff IPs	Authen	Sn Lifespan	Anti-GPS	ID Lifespan	PII
Uber	●	○	●	∞	○	∞	●
Easy	-	○	○	∞	○	∞	●
Gett	-	○	●	∞	○	∞	●
Lyft	●	○	●	24h	○	∞	○
myTaxi	-	○	○	∞	○	20m	●
Taxify	●	○	●	∞	○	∞	●
BiTaksi	-	○	●	∞	○	∞	●
Heetch	-	○	●	∞	○	∞	●
Jeeny	-	○	○	∞	○	20m	●
Flywheel	-	○	●	20m	○	10m	●
GoCatch	-	○	●	∞	○	∞	●
miCab	-	○	●	∞	○	∞	○
RideAustin	-	○	●	∞	○	∞	●
Ztrip	-	○	●	30m	○	∞	●
eCab	●	○	○	∞	○	∞	●
GroundLink	-	○	○	∞	○	∞	●
HelloCabs	-	○	●	∞	○	∞	○
Ride LA	-	○	○	∞	○	∞	○
Bounce	-	○	●	∞	○	∞	○
DC Taxi Rider	-	○	●	∞	○	∞	○

Summary

- 1 No Particular Countermeasures Implemented
- 2 Six Services Do Not Require User Authentication
- 3 Six Services Directly Return A Variety of PII

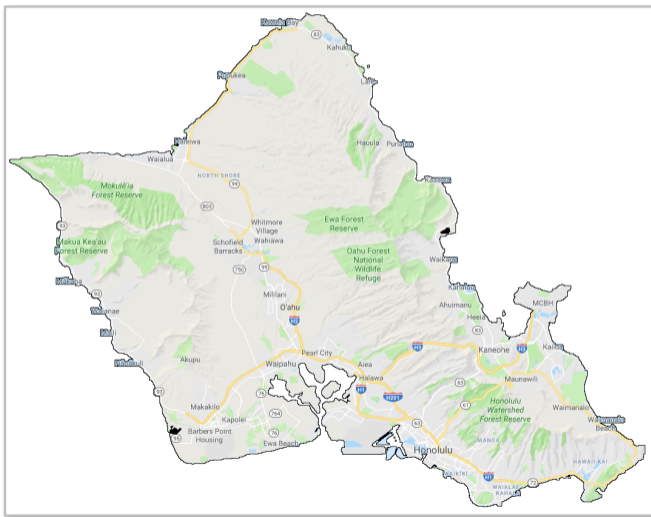
Data Acquisition: Selecting City



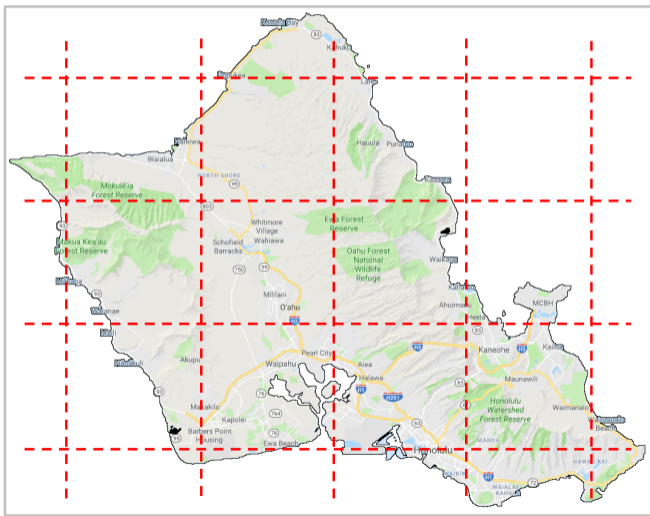
Data Acquisition: Selecting City



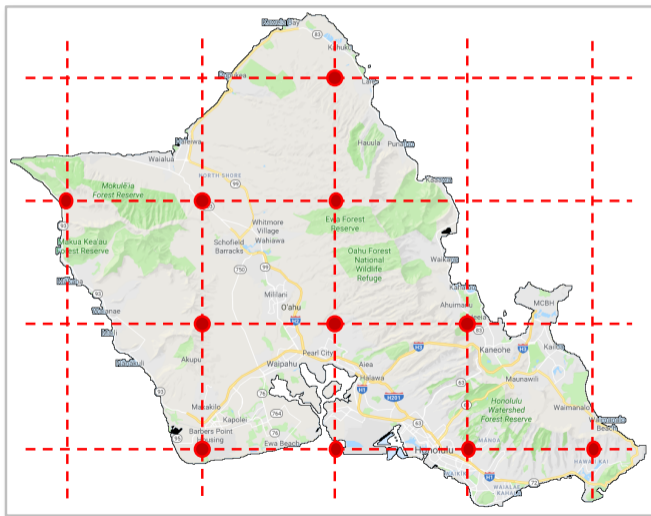
Data Acquisition: Placing Monitors



Data Acquisition: Placing Monitors



Data Acquisition: Placing Monitors



The Answers to Research Questions

The Research Questions

- ① Private Info Leakage
 - ▶ Direct PII of Drivers
 - ▶ Movement of Drivers
 - ▶ Working Patterns of Drivers
 - ▶ Appeared Locations of Drivers
- ② Business Info Leakage
 - ▶ Dual-Apping Driver
 - ▶ Driver Preference
 - ▶ # Drivers
 - ▶ Operation Performance

The Answers to Research Questions

The Research Questions

- 1 Private Info Leakage
 - ▶ Direct PII of Drivers
 - ▶ Movement of Drivers
 - ▶ Working Patterns of Drivers
 - ▶ Appeared Locations of Drivers
- 2 Business Info Leakage
 - ▶ Dual-Apping Driver
 - ▶ Driver Preference
 - ▶ # Drivers
 - ▶ Operation Performance

Confirmed Vulnerabilities

- 1 Private Info Leakage
 - ▶ Direct PII of Drivers ✓
 - ▶ Movement of Drivers ✓
 - ▶ Working Patterns of Drivers ✓
 - ▶ Appeared Locations of Drivers ✓
- 2 Business Info Leakage
 - ▶ Dual-Apping Driver ✓
 - ▶ Driver Preference ✓
 - ▶ # Drivers ✓
 - ▶ Operation Performance ✓

(I). Private Information Leakage : Direct PII Leakage

Service name	Sensitive information
Lyft	Driver avatar
HelloCabs	Name , phone number
Ride LA	Name, phone number
DC Taxi Rider	Name, phone number, email
miCab	Account creating time, account last update time, device number, hiring status
Bounce	Name, date of birth, driver avatar, phone number, social security number , driver license number , driver license expiration date, home address , bank account number , routing number, account balance, vehicle inspection details, vehicle insurance details

(I). Private Information Leakage: Movements of Drivers



(I). Private Information Leakage: Appeared Locations → Home

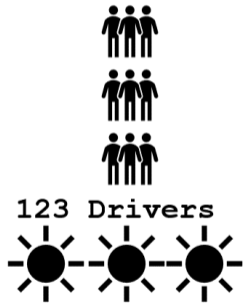
(I). Private Information Leakage: Appeared Locations → Home



334 Drivers



(I). Private Information Leakage: Appeared Locations → Home



(I). Private Information Leakage: Appeared Locations → Home



(I). Private Information Leakage: Appeared Locations → Home

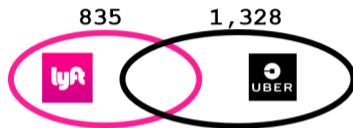


(II). Business Info Leakage - Dual App-ing Drivers

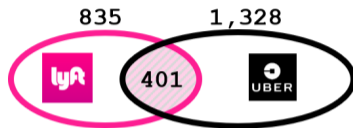
835



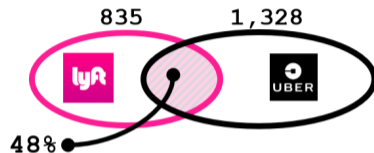
(II). Business Info Leakage - Dual App-ing Drivers



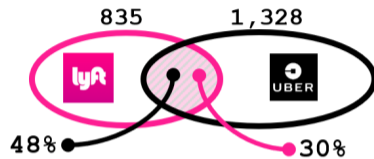
(II). Business Info Leakage - Dual App-ing Drivers



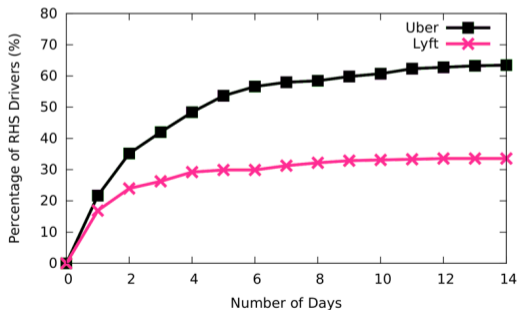
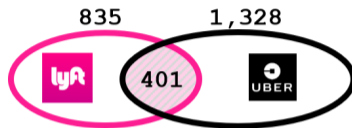
(II). Business Info Leakage - Dual App-ing Drivers



(II). Business Info Leakage - Dual App-ing Drivers



(II). Business Info Leakage - Dual App-ing Drivers



Discussions

Suggestions

- ① Appropriate Implementation Logic
 - ▶ No PII before Service Reservation
- ② Concealing Position with Distance
 - ▶ Replacing Car Position with Distance to Riders
- ③ Mitigating **Linkability**
 - ▶ Removing or Using Short-live Car IDs

Discussions

Suggestions

- 1 Appropriate Implementation Logic
 - ▶ No PII before Service Reservation
- 2 Concealing Position with Distance
 - ▶ Replacing Car Position with Distance to Riders
- 3 Mitigating **Linkability**
 - ▶ Removing or Using Short-live Car IDs

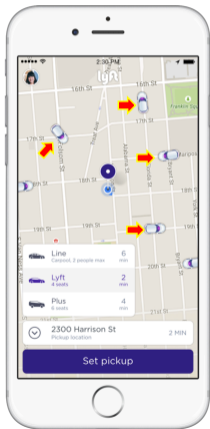
Responsible Disclosure

- 1 Disclosure to all 20 Apps
- 2 8 Responded and Started Fixing: removing PII, using short-live IDs, ...
- 3 Two Bug Bounties from **Uber** and **Lyft**

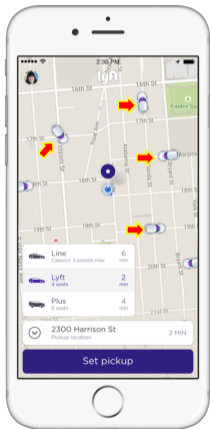
Related Work

- 1 **Privacy-Preserving Location-Based Services (LBS):** [LKZM08], [HLR11], [ZC11], [LH10], ORide [PDE⁺17] and PrivateRide [PDJ⁺17].
- 2 **Leakage of Privacy Sensitive Data in Mobile Applications:** TaintDroid. [EGC⁺10], Appintent. [YYZ⁺13], PiOS. [EKKV11], SUPOR [HLX⁺15], UiRef [AAL⁺17], [JHY⁺14], [FHM⁺12], [MDM⁺15], [KCE⁺17], AuthScope [ZZL17], and LeakScope [ZLZ19].
- 3 **Web API and Protocol Reverse Engineering:** [CKW07], [PI], [CS07], AutoFormat [LJXZ08], Dispatcher [CPKS09], Reformat [WJC⁺09], and WARDroid [MG18].
- 4 **Dynamic Analysis of Mobile Apps:** TaintDroid [EGC⁺10], AppsPlayground [RCE13], DECAF [LNGL14], and SmartGen [ZL17].

Summary: The Security with The Nearby Cars API



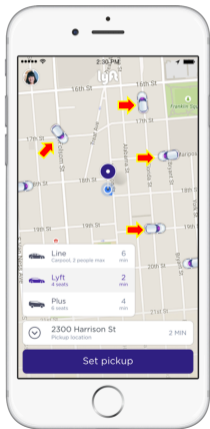
Summary: The Security with The Nearby Cars API



Summary

- 1 In-depth Study of Ride-Hailing Services
 - ▶ Top 20 Suggested Ride-Hailing Apps
 - ▶ World-wide Known
- 2 No Particular Countermeasure for Data Scraping
 - ▶ No defense for Diff IPs, GPS Spoofing
 - ▶ Few uses short-live session & identifier

Summary: The Security with The Nearby Cars API



Summary

- 1 In-depth Study of Ride-Hailing Services
 - ▶ Top 20 Suggested Ride-Hailing Apps
 - ▶ World-wide Known
- 2 No Particular Countermeasure for Data Scraping
 - ▶ No defense for Diff IPs, GPS Spoofing
 - ▶ Few uses short-live session & identifier

Confirmed Vulnerabilities

- 1 **Private Info Leakage**
 - ▶ Direct PII of Drivers ✓
 - ▶ Movement of Drivers ✓
 - ▶ Working Patterns of Drivers ✓
 - ▶ Appeared Locations of Drivers ✓
- 2 **Business Info Leakage**
 - ▶ Dual-Apping Driver ✓
 - ▶ Driver Preference ✓
 - ▶ # Drivers ✓
 - ▶ Operation Performance ✓

Thank You

Geo-locating Drivers: A Study of Sensitive Data Leakage in Ride-Hailing Services

Qingchuan Zhao*, Chaoshun Zuo*, Giancarlo Pellegrino^{†‡}, Zhiqiang Lin*

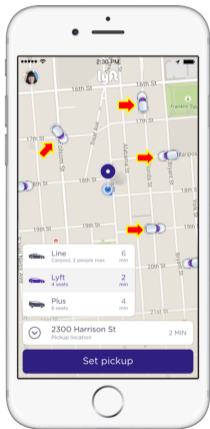
*The Ohio State University

†CISPA Helmholtz Center for Information Security

‡Stanford University

NDSS 2019

Take Away: The Security with The Nearby Cars API









Summary

- 1 In-depth Study of Ride-Hailing Services
 - ▶ Top 20 Suggested Ride-Hailing Apps
 - ▶ World-wide Known
- 2 No Particular Countermeasure for Data Scraping
 - ▶ No defense for Diff IPs, GPS Spoofing
 - ▶ Few uses short-live session & identifier

Confirmed Vulnerabilities

- 1 **Private Info Leakage**
 - ▶ Direct PII of Drivers ✓
 - ▶ Movement of Drivers ✓
 - ▶ Working Patterns of Drivers ✓
 - ▶ Appeared Locations of Drivers ✓
- 2 **Business Info Leakage**
 - ▶ Dual-Apping Driver ✓
 - ▶ Driver Preference ✓
 - ▶ # Drivers ✓
 - ▶ Operation Performance ✓









References I

-  Benjamin Andow, Akhil Acharya, Dengfeng Li, William Enck, Kapil Singh, and Tao Xie, *Uiref: Analysis of sensitive user inputs in android applications*, Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (New York, NY, USA), WiSec '17, ACM, 2017, pp. 23–34.
-  Weidong Cui, Jayanthkumar Kannan, and Helen J. Wang, *Discoverer: Automatic protocol reverse engineering from network traces*, Proceedings of the 16th USENIX Security Symposium (Security'07) (Boston, MA), August 2007.
-  Juan Caballero, Pongsin Poosankam, Christian Kreibich, and Dawn Song, *Dispatcher: Enabling active botnet infiltration using automatic protocol reverse-engineering*, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS'09) (Chicago, Illinois, USA), 2009, pp. 621–634.
-  Juan Caballero and Dawn Song, *Polyglot: Automatic extraction of protocol format using dynamic binary analysis*, Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07) (Alexandria, Virginia, USA), 2007, pp. 317–329.
-  William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth, *Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones*, Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (Berkeley, CA, USA), OSDI'10, USENIX Association, 2010, pp. 393–407.
-  Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna, *PiOS : Detecting privacy leaks in iOS applications*, NDSS 2011, 18th Annual Network and Distributed System Security Symposium, 6-9 February 2011, San Diego, CA, USA (San Diego, UNITED STATES), 02 2011.





References II

-  Sascha Fahl, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben, and Matthew Smith, *Why eve and mallory love android: An analysis of android ssl (in)security*, Proceedings of the 2012 ACM Conference on Computer and Communications Security (New York, NY, USA), CCS '12, ACM, 2012, pp. 50–61.
-  Wenbo He, Xue Liu, and Mai Ren, *Location cheating: A security challenge to location-based social network services*, Distributed Computing Systems (ICDCS), 2011 31st International Conference on, June 2011, pp. 740–749.
-  Jianjun Huang, Zhichun Li, Xusheng Xiao, Zhenyu Wu, Kangjie Lu, Xiangyu Zhang, and Guofei Jiang, *Supor: Precise and scalable sensitive user input detection for android apps.*, USENIX Security Symposium, 2015, pp. 977–992.
-  Xing Jin, Xuchao Hu, Kailiang Ying, Wenliang Du, Heng Yin, and Gautam Nagesh Peri, *Code injection attacks on html5-based mobile apps: Characterization, detection and mitigation*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (New York, NY, USA), CCS '14, ACM, 2014, pp. 66–77.
-  William Koch, Abdelberi Chaabane, Manuel Egele, William Robertson, and Engin Kirda, *Semi-automated discovery of server-based information oversharing vulnerabilities in android applications*, Proceedings of the 26th ACM SIGSOFT International Symposium on Software Testing and Analysis, ACM, 2017, pp. 147–157.
-  Wanying Luo and Urs Hengartner, *Veriplace: A privacy-aware location proof architecture*, Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems (New York, NY, USA), GIS '10, ACM, 2010, pp. 23–32.
-  Zhiqiang Lin, Xuxian Jiang, Dongyan Xu, and Xiangyu Zhang, *Automatic protocol format reverse engineering through context-aware monitored execution*, Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08) (San Diego, CA), February 2008.

References III

-  Vincent Lenders, Emmanouil Koukoumidis, Pei Zhang, and Margaret Martonosi, *Location-based trust for mobile user-generated content: Applications, challenges and implementations*, Proceedings of the 9th Workshop on Mobile Computing Systems and Applications (New York, NY, USA), HotMobile '08, ACM, 2008, pp. 60–64.
-  Bin Liu, Suman Nath, Ramesh Govindan, and Jie Liu, *Decaf: Detecting and characterizing ad fraud in mobile apps*, Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation (Berkeley, CA, USA), NSDI'14, USENIX Association, 2014, pp. 57–70.
-  Patrick Mutchler, Adam Doupé, John Mitchell, Chris Kruegel, and Giovanni Vigna, *A large-scale study of mobile web app security*, Proceedings of the Mobile Security Technologies Workshop (MoST), 2015.
-  Abner Mendoza and Guofei Gu, *Mobile application web api reconnaissance: Web-to-mobile inconsistencies and vulnerabilities*, Proceedings of the 39th IEEE Symposium on Security and Privacy (SP'18), May 2018.
-  Anh Pham, Italo Dacosta, Guillaume Endignoux, Juan Ramon Troncoso Pastoriza, Kevin Huguenin, and Jean-Pierre Hubaux, *Oride: A privacy-preserving yet accountable ride-hailing service*, 26th USENIX Security Symposium (USENIX Security 17) (Vancouver, BC), USENIX Association, 2017, pp. 1235–1252.
-  Anh Pham, Italo Dacosta, Bastien Jacot-Guillarmod, Kévin Huguenin, Taha Hajar, Florian Tramèr, Virgil D. Gligor, and Jean-Pierre Hubaux, *Privateride: A privacy-enhanced ride-hailing service*, PoPETs 2017 (2017), no. 2, 38–56.
-  *The Protocol Informatics Project*, <http://www.baselineresearch.net/PI/>.
-  Vaibhav Rastogi, Yan Chen, and William Enck, *Appsplayground: Automatic security analysis of smartphone applications*, Proceedings of the Third ACM Conference on Data and Application Security and Privacy (New York, NY, USA), CODASPY '13, ACM, 2013, pp. 209–220.

References IV

-  Zhi Wang, Xuxian Jiang, Weidong Cui, Xinyuan Wang, and Mike Grace, *Reformat: Automatic reverse engineering of encrypted messages*, Proceedings of 14th European Symposium on Research in Computer Security (ESORICS'09) (Saint Malo, France), LNCS, September 2009.
-  Zhemin Yang, Min Yang, Yuan Zhang, Guofei Gu, Peng Ning, and X. Sean Wang, *Appintent: Analyzing sensitive data transmission in android for privacy leakage detection*, Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (New York, NY, USA), CCS '13, ACM, 2013, pp. 1043–1054.
-  Zhichao Zhu and Guohong Cao, *Applaus: A privacy-preserving location proof updating system for location-based services*, INFOCOM, 2011 Proceedings IEEE, April 2011, pp. 1889–1897.
-  Chaoshun Zuo and Zhiqiang Lin, *Exposing server urls of mobile apps with selective symbolic execution*, Proceedings of the 26th World Wide Web Conference (WWW'17) (Perth, Australia), April 2017.
-  Chaoshun Zuo, Zhiqiang Lin, and Yinqian Zhang, *Why does your data leak? uncovering the data leakage in cloud from mobile apps*, Proceedings of the 2019 IEEE Symposium on Security and Privacy (San Francisco, CA), May 2019.
-  Chaoshun Zuo, Qingchuan Zhao, and Zhiqiang Lin, *Authscope: Towards automatic discovery of vulnerable authorizations in online services*, Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS'17) (Dallas, TX), November 2017.