CLOUD SEEDING

ЩНО??

GRAEME NEILSON

GRAEME@LOLUX.NET

VLADIMIR WOLSTENCROFT

VLADIMIR.WOLSTENCROFT@GMAIL.COM

WHAT?

- ABUSING CROWD SOURCE SERVICES USING CLOUD SERVICES
- BOTS VERSUS HUMANS IN THE CROWD CLOUD
- REVERSE ENGINEERING PRINCIPLES APPLIED TO THE CLOUD

CAN WE MAKE IT RAIN??

- HOW DO WE TEST OUR CLOUD SEEDING THEORIES?
- THERE ARE NO VMS OR TRIAL APPS...
- CAN WE CONTROL CROWD SOURCED CLOUD SYSTEMS REAL-TIME, ON DEMAND?

UBER

- FREE RIDES
- TRACKING DRIVERS
- CONTROL DRIVERS
- CONTROL PRICING
- DENIAL OF SERVICE

UBER

- AVAILABLE WORLDWIDE
- RELEASING PUBLIC API
- STILL USES PRIVATE API
- PROMOTIONAL SYSTEM

TOP SECRET

- DATA COLLECTION ON USERS:

  HTTPS://WEB.ARCHIVE.ORG/WEB/20140827195715/HTTP://BLOG.UBER.COM/RIDESOFGLORY

- NON-TRANSPARENT PRICE SURGING

- CERTIFICATE PINNING PREVENTS PROXY

- OBFUSCATED CODE ONCE DECOMPILED

REV3RSING

- DEVELOPER LEFT DEBUG CODE AND TEST CODE
- RESOURCES.ARSC
- CERTIFICATE PINNING
- API KEYS AND MESSAGE TYPES

HEISENBERG

source.mVehiclePhotoUrl =
"https://uber-mobile.s3.amazonaws.com/android-notification-testing/bounder.jpg";
source.mVehicleMake = "Fleetwood";
source.mVehicleModel = "Bounder";
source.mVehicleLicense = "COOK";
source.mDriverName = "Heisenberg";
source.mDriverPhotoUrl =
“https://uber-mobile.s3.amazonaws.com/android-notification-testing/heisenberg.jpg";

SECRETS REVEALED

BYPASSING CERTIFICATE PINNING

- FIND SSLSOCKET FACTORY CALL (GREP AND STRINGS)
- FIND THE CALL TO OPEN THE BINARY KEY STORE (BKS)
- PASSWORD FOR BKS MUST BE IN APP AND PASSED IN CALL
- USE ANDROID KEYTOOL TO INSERT ANOTHER CERTIFICATE INTO THE BKS
- GENERATE A SELF SIGNED CERTIFICATE TO RE-SIGN THE APPLICATION
- SIDE LOAD THE RE-SIGNED APP ON MOBILE
- PROXY AND CAPTURE REST API REQUESTS AND RESPONSES

KEYSTORE

```
#!/bin/sh

echo " -- Keystore Fixer -- "
echo "UBER KEYSTORE PASSWORD"
echo "sMdqVqJBdBmmkDMp6BK7EVeEkHcNbJ"

#insert burp cert into keystore
keytool -provider org.bouncycastle.jce.provider.BouncyCastleProvider -storetype
BKS -keystore ssl_pinning_certs_bk146.bks -importcert -v trustcacerts -file
burp.der -alias burp

read -n "Delete Uber certificates from the apk META-INF directory"

# sign apk
jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore
cloudseed.keystore Uber-burp.apk cloudseed.cert

# verify apk
jarsigner -verify -verbose -certs Uber-burp.apk
```

PROXY RIDING

TAKE AN UBER WITH SOME "LUGGAGE"

1. PHONE RUNNING UBER APP CONNECTED TO HOTPSOT
2. HOTSPOT PHONE FOR LOCAL WIFI TO 3G
3. LAPTOP PROXYING UBER TO HOTSPOT

BONUS POINTS: CHAT WITH UBER DRIVER TO FIND OUT AS MUCH AS POSSIBLE ABOUT HOW THEIR DRIVER APP WORKS

TAXI TRACKING

- GAIN ADMIN MODE BY EDITING RESPONSE IN BURP
- BIG JSON: LOTS OF DATA TRACKED: PHONE, CARRIER, CHARGING, BATTERY STATUS, LAST ACTION, WIFI STATUS, LOCAL IP
- LYFT TRACKS IF YOU USE UBER...

UBER

TRACKING DRIVERS

GEO TRACKING

- POSSIBLE TO TRACK JUST LIKE THE APP, BUT ALSO:
  - TRACK DRIVER ID'S OVER TIME
  - ASSOCIATE ID'S WITH DRIVERS WHEN REQUESTING RIDES
  - CALCULATE SPEED OF DRIVERS
  - GET NUMBER OF AVAILABLE DRIVERS

UBER

FREE RIDES

PROMOTIONS

NO MEANINGFUL EXPLOITATION IN THE TRADITIONAL SENSE

EASIEST WAY TO GAIN FREE RIDES...

https://cn-dc1.uber.com/validate/promotion?promotion_code=234&confirmed=1

{"new_clients_only": true, "promotion_value_string": "$20 off first ride", "country_iso2": "US", "give_get_amount": "$20", "description": "$20 off your first ride! "}

{"promotion_value_string": "￥10 off first 3 rides", "country_iso2": "CN", "give_get_receiver_headline": "Sign up now to claim your free gift from 1 (￥10 off first 3 rides)*.", "inviter": {"first_name": "1"}, "give_get_amount": "￥10"}

RIDE SHARING

ONCE AN ACCOUNT IS CREATED

- TAKE RIDES AFTER ADDING PAYMENT METHODS
- USE REFER CODES TO GET $10 DOLLAR FREE RIDE AND REFER TO ACCOUNT OF CHOICE $10
- ADD SPECIAL CODES TO GET DISCOUNTS

THE SOCIALIST WAY

RIDE SHARING FOR FREE

PROMOTION ABUSE REQUIRES MASS ACCOUNT CREATION TO BE USEFUL

FIRST NEED TO PROVE AUTOMATED SINGLE ACCOUNT CREATION

PROBLEMS

- ACCOUNT CREATION REQUIRES ENCRYPTED PAYMENT DATA
  - USE BRAIN PUBLIC KEY TO CREATE ENCRYPTED DATA FOR ACCOUNT
- ACCOUNT NEEDS TO BE VERIFIED POST SIGN UP
  - VERIFICATION USING 4 DIGIT PIN SENT VIA SMS TO MOBILE
  - PIN RESET AFTER 4 INCORRECT ATTEMPTS

ME, MYSELF AND MY PHONE

"WE ARE PASSED THE POINT OF USERNAMES, IT'S REAL IDS NOW ATTACHED TO EVERY ACCOUNT. THEY WANT OUR REAL NAMES, CELL PHONE NUMBERS, PERSONAL INFORMATION AND BANKING INFORMATION LINKED TO ALL OUR ACCOUNTS – PHONES ARE SEEN AS A WAY TO DO THIS"

...NEED TO FIND A WAY TO BYPASS OR DO VERIFICATION..

WRONG NUMBERS

- CROWD /CLOUD APPS CONFUSE PHONES WITH HUMANS
- THEY ASSUME THE PHONE IS A CLOSED DEVICE SUITABLE FOR KEEPING SECRETS
- THEY ASSUME THEIR API WILL ONLY BE USED BY THE OFFICIAL CLIENT APP ON A MOBILE DEVICE

BYPASS VERIFICATION?

NEED TO INTERACT WITH THE API BY EITHER BYPASSING MOBILE VERIFICATION OR API ACCESS TO MANY PHONE NUMBERS...

BYPASS VERIFICATION?

POSSIBLE TO SEND VERIFICATION TO OTHER PHONES:

{"country_iso2":"NZ","locale":"en","strategy":"default_verification","user_uuid":"bbc2ad57-7f41-4b5f-91ce-eaa0e5964503"}

EVEN POSSIBLE TO PERFORM VOICE VERIFICATION FOUND ON SOURCE CODE (ALLOWS TO VERIFY ON LAND LINES AND SKYPE NUMBERS ☺)

{"country_iso2":"NZ","locale":"en","strategy":"voice_verification","user_uuid":"bbc2ad57-7f41-4b5f-91ce-eaa0e5964503"}

BUT SKYPE NUMBERS ARE EXPENSIVE..

ANOTHER WAY??

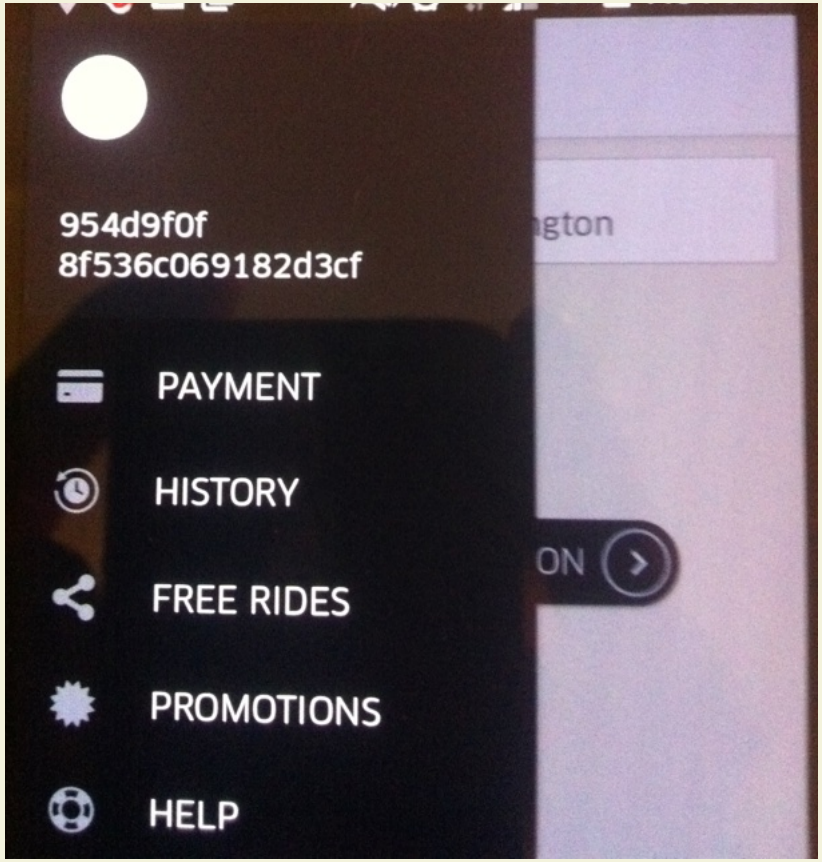
LINKING MACHINES

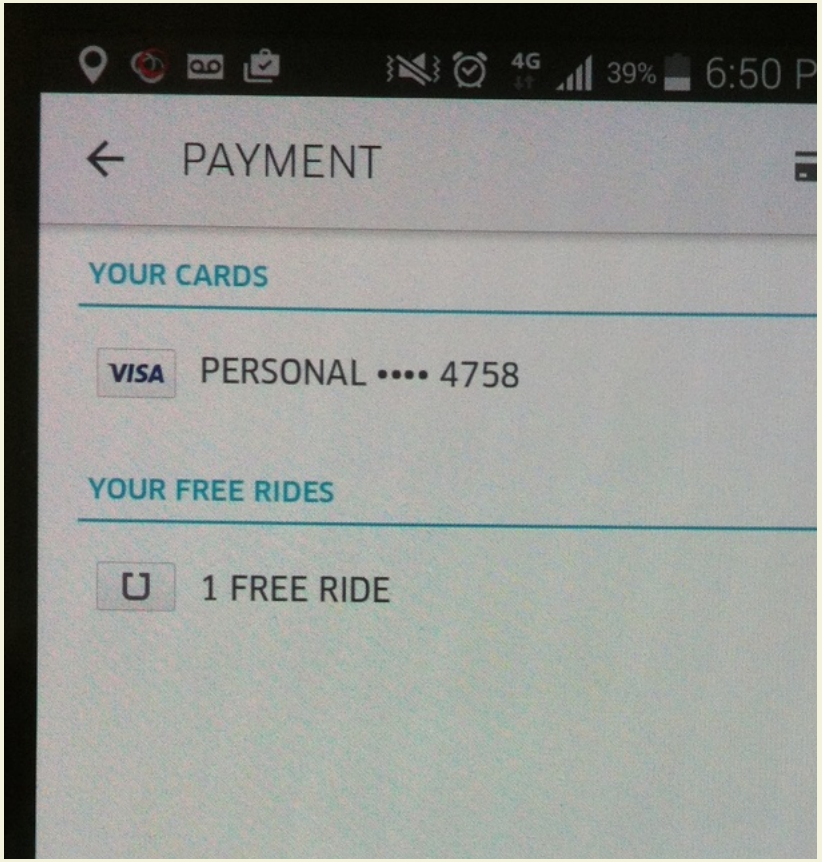
- GLOBAL MOBILE AND LANDLINE NUMBERS
- NUMBER LOOKUP INFORMATION
- API VIA PYTHON, RUBY, PHP FOR TELEPHONY
- SMS SEND AND RECEIVE

TWILIO

- CLOUD BASED API FOR NUMBER GENERATION AND TELEPHONY SERVICES
- CHEAP NUMBERS $1/MONTH
- OFFSET PHONE COSTS THROUGH PROMOTIONS.
- CAN EASILY CREATE THOUSANDS OF NUMBERS
- UBER USE TWILIO :-)

RIDE SHARING...





THE SOCIALIST WAY

ACCOUNT CREATION...

THE SOCIALIST WAY

OFFSETING COSTS

EACH NUMBER CAN BE USED FOR A MASSIVE VARIETY OF SERVICES WHICH USE PHONES TO VERIFY YOU...

JUST A FEW ARE:

- ORDERUP
- TINDER
- TWITTER
- HAPPN
- FACEBOOK - PIN TO RESET PASSWORD
- PLSPLSME
- MCENT
- LINK MESSENGER
- GLIDE
- TENCENT
- TANGO
- HUSHMAIL
- STEAM
- FLYP
- EQUINENOW.COM
- NOBELAPP - PIN TO RESET PASSWORD

SOCIALIST ACCOUNT CREATION

SO FAR IT HAS COST $1–$5 TO CREATE EACH ACCOUNT

EVEN THOUGH WE CAN OFFSET ACCOUNT CREATION IT SHOULD BE ZERO COST...

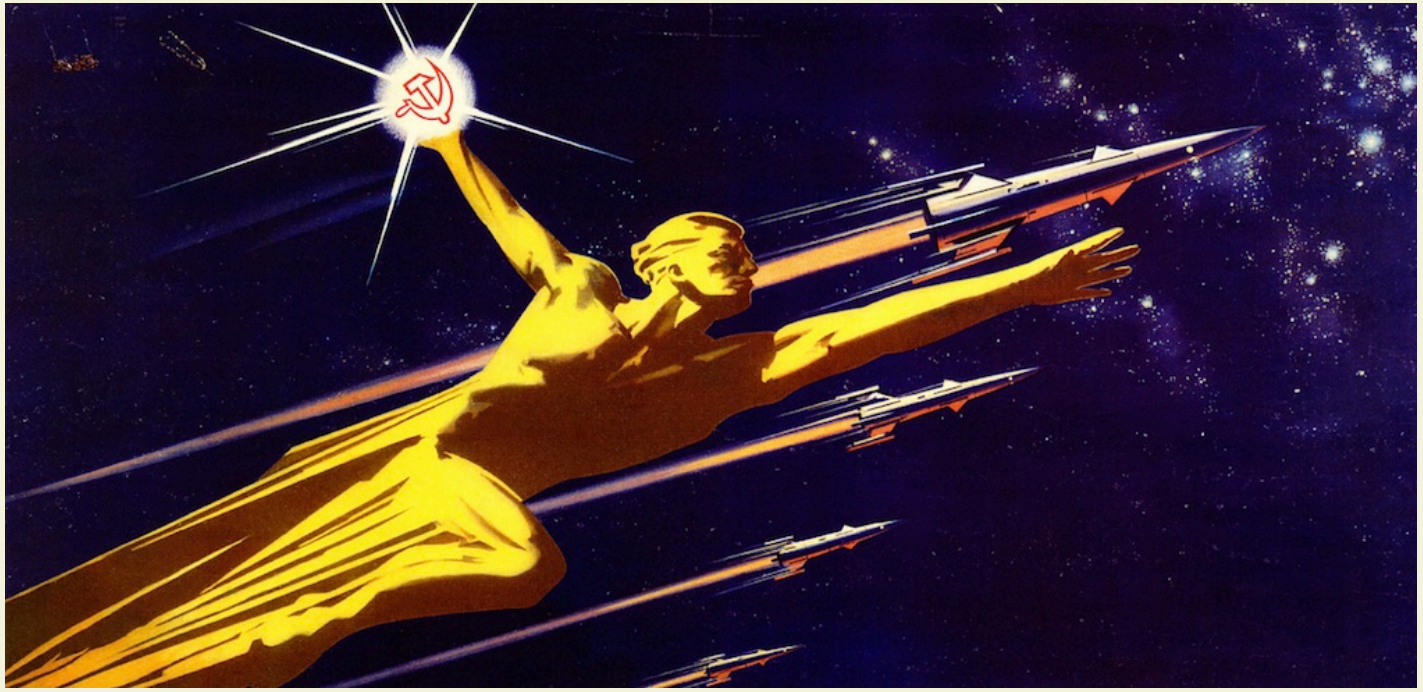
THERE MUST BE A BETTER WAY...

LAUNCHING SEEDERS

- PHONE VALIDATION OCCURS AFTER ACCOUNT CREATION
- 4 TRIES BEFORE PIN IS RESET
- FOR ZERO COST ALL WE NEED TO DO IS GUESS THE PIN...

MAKING IT RAIN

CAN WE LAUNCH A HORIZONTAL BRUTE-FORCE ATTACK TO GUESS VERIFICATION PINS?



CREATE 10,0000 ACCOUNTS AND TRY A PIN AGAINST THEM ALL

CROWD OF ROBOTS

CREATE ACCOUNTS

CREATED AROUND 20,000 UBER ACCOUNTS

- RANDOM TIME WAITS
- MULTI THREADED
- RANDOMISED DATA
- ENCRYPTED PAYMENTS
- LOTS OF PHONE NUMBERS (LANDLINE NUMBERS)

BRUTE FORCE

- **AGAINST ACCOUNTS FROM DIFFERENT COUNTRIES:**
  - **SEND REQUEST WITH SMS:**

```
{"locale": "en", "country_iso2": "DE", "user_uuid":
"ecb434c6-05aa-4437-8081-4a0548264a27", "strategy":
"default_verification"}
```

  - **SEND 4 TOKENS:**

```
{"mobileToken": "1668"}
```

2 ACCOUNTS IN 90 SECS FROM 1000 ACCOUNTS

HERE COMES THE RAIN

- FREE SHORT DISTANCE RIDES VIA THROWAWAY ACCOUNTS (PREVENTS TRACKING)
- PUMP REFERRER PROMOTION TO ONE DISPOSABLE ACCOUNT FOR LONGER RIDES
- TRACK DRIVERS: HOMES, PLATES, PHOTOS, SPEED

TORRENTIAL RAIN

- USE ACCOUNTS TO CAUSE SURGE PRICING
- MOVE ALL THE CARS TO SPECIFIC LOCATIONS
- BOOK ALL THE CARS WITH ROBOTS
- REGISTER ALL THE MOBILE NUMBERS

LYFT

LYFT : MADE IN AMERICA

PHONE SHARING

- SHARED US NUMBERS ARE AVAILABLE ONLINE FOR FREE
- ATTEMPTING TO USE THESE FOR UBER ACCOUNTS JUST RETURNS AN ERROR AS ALL THESE NUMBERS ARE REGISTERED
- BUT ON LYFT USE A SHARED US NUMBER TO GET PIN?
- GOOGLE "LYFT CODE"?

YOUR LYFT CODE IS:

Lyft - Receive SMS Online
receive-sms.com/messages.php?tag=Lyft
14804058046 · 14079022246, **Your Lyft code is** 6824, 1 month ago. 14804058046 · 14079022246, This is Lyft. Please enter the verification code you received ...

LYFT - Receive SMS Online
articulo.receive-sms.com/index.php?tag=LYFT
14804058046 · 14079022246, **Your Lyft code is** 6824, 3 weeks ago. 14804058046 · 14079022246, This is Lyft. Please enter the verification code you received ...

Received a text message "Your Lyft code is.... - Corvette Forum
www.corvetteforum.com/.../3614354-received-a-text-mes... CorvetteForum
Mar 1, 2015 - Posts: 18,507. Location: Sussex,Wi. Thanks: 0. Thanked 3 Times in 3 Posts. Default Received a text message "**Your Lyft code is**.

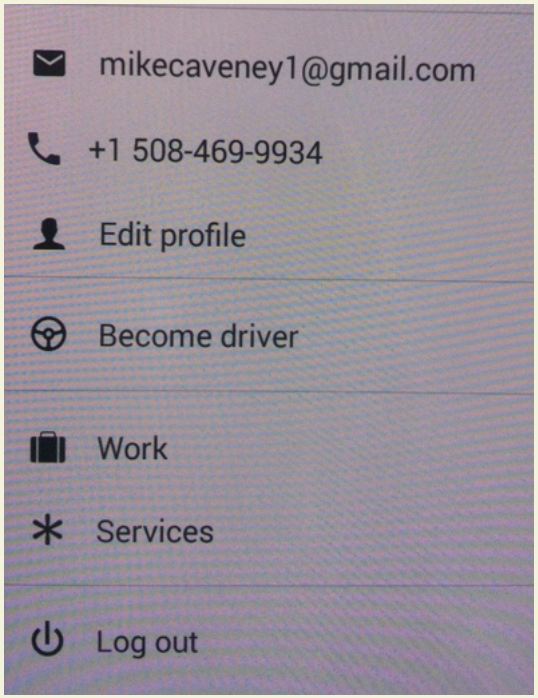
Receive 16133192839(USA) SMS Online For Free
hs3x.com/read-sms-16133192839.html
15107688751, **Your Lyft code is** 4454 Phone Verification Service for WhatsApp, Facebook,Instagram,Naver, Twitter, Craigslist...==>CLICK HERE, 6 hours ago.

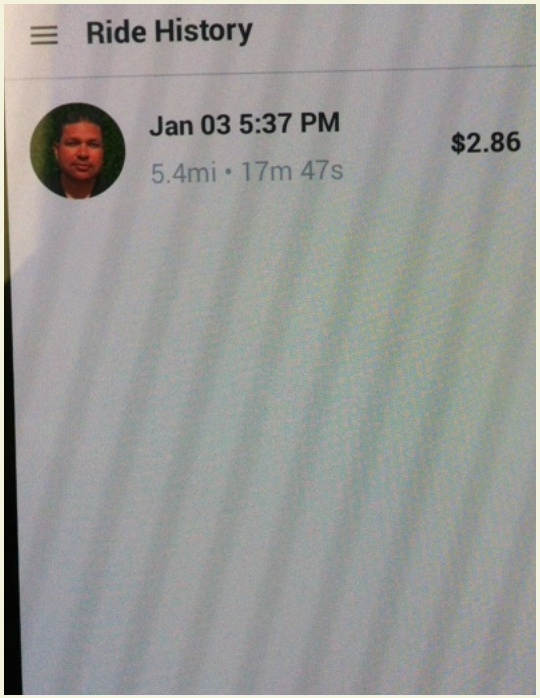
Receive SMS Verification - Messages received for + ...
receivesmsverification.com/+19132148403.php
Circle verification code: 797333. United-States. +13136517592. 1 year ago. Circle: 456982. Unknown. 46080. 1 year ago. **Your Lyft code is** 9873. Unknown.

Free SMS Verification - Incoming SMS Online - Receive SMS
freesmsverification.com/+19133254296.php
+17047548886, 4 weeks ago, **Your Lyft code is** 7826. +16046704874, 4 weeks ago ... +17047548886, 2 months ago, **Your Lyft code is** 5245. +17047548886, 2 ...

PHONE SHARING

ACCOUNTS WITH SHARED PHONE NUMBERS ARE ALREADY REGISTERED BUT...



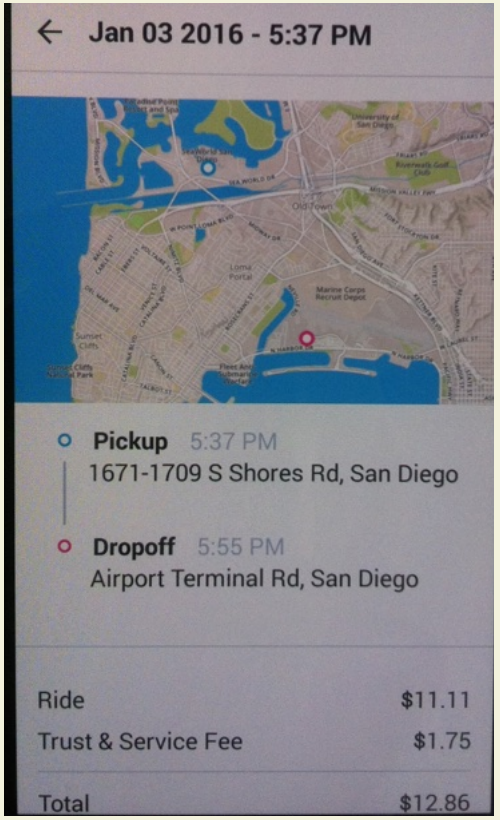


THE SOCIALIST WAY

PHONE SHARING

ACCESS TO TRIP HISTORY ONCE AUTHENTICATED AS ANOTHER USER..

POSSIBLE TO TRACK THESE SHARED PHONE USERS



THE SOCIALIST WAY

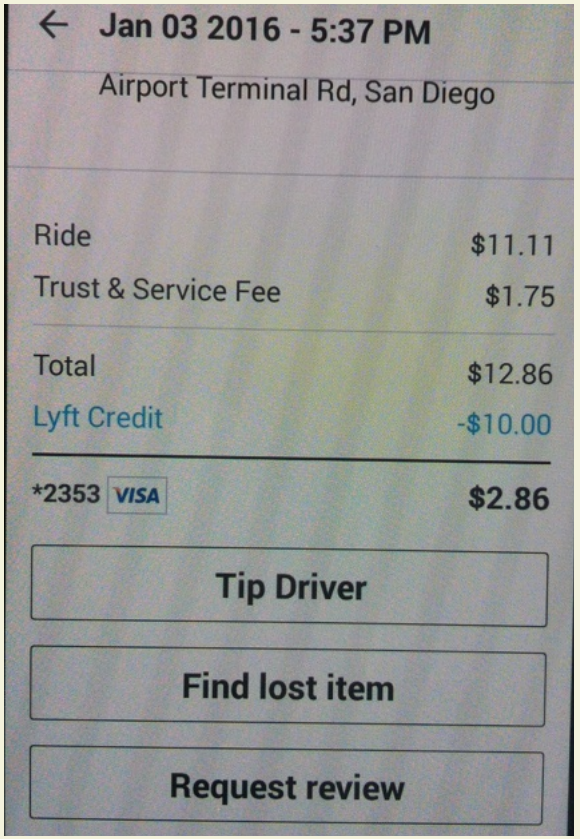
PHONE SHARING

ACCESS TO TRIP HISTORY ONCE AUTHENTICATED AS ANOTHER USER

POSSIBLE TO TRACK THESE SHARED PHONE USERS

...

AND TIP DRIVERS USING THEIR PAYMENT METHODS..



THE SOCIALIST WAY

PHONE SHARING

ACCESS TO TRIP HISTORY ONCE AUTHENTICATED AS ANOTHER USER

POSSIBLE TO TRACK THESE SHARED PHONE USERS

...

AND RESUME THEIR DRIVER APPLICATION...

THE SOCIALIST WAY

HERE COMES THE RAIN AGIAN

APPLYING THE PREVIOUS BRUTE FORCE TECHNIQUES:

LYFT ONLY REQUIRES 2 UN-AUTHENTICATED REQUESTS:

- DELIVER SMS TOKEN TO MOBILE
- SEND LOGIN OR SIGNUP REQUEST
- 15 ATTEMPTS ALLOWED PER NUMBER
- TOKEN ASSOCIATED FOR 48 HOURS AND IS RE-PLAYABLE

HEAVY DOЩИРОЦЯ

- RIDE HISTORY (TARGETED ATTACK)
- MOBILE USER ENUMERATION
- IMPERSONATE DRIVERS - SINCE IT'S A SINGLE APP!!
- INFORMATION COMPROMISE:
  - PHONE NUMBER, EMAIL, ADDRESS, LAST 4 DIGITS OF CREDIT CARD

CLOUD BOTS

VERIFICATION USING PIN CODES DELIVERED TO PHONES IS VERY WEAK SECURITY - WE KNEW THIS...

ALL CARS CAN BE SENT TO SPECIFIC LOCATIONS BY ROBOTS

ALL THE CARS CAN BE TAKEN BY ROBOTS ALL THE TIME

ALL THE MOBILE NUMBERS COULD BE REGISTERED BY ROBOTS