

Turning a GPS-based dating application into a tracking system

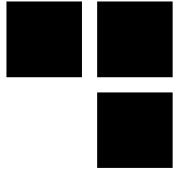


When 13/05/2017

Where ESE ESIEA 2017

Who Julien Legras (@Julien_Legras) & Julien Szlamowicz (@szLam_)





About us

- **Julien Legras & Julien Szlamowicz**
 - Synacktiv Ninjas
 - ESIEA Badge trainers



Synacktiv



- **Pentests**
- **Audits**
- **Red Team**
- **Vulnerability research**
- **Training classes**
- **Consulting**

Big brother



- Big brother is watching you

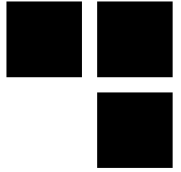




Many ways to perform GPS tracking

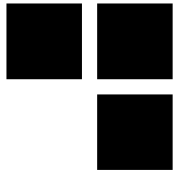


- **2016 – Ben Zhao - University of California Santa Barbara**
- **Scan an arbitrary rectangular zone**
 - Return verbose information about people in the zone
 - Exact location
- **Deploy a 20 probes grid around the target**
- **Center the grid after every target location update**

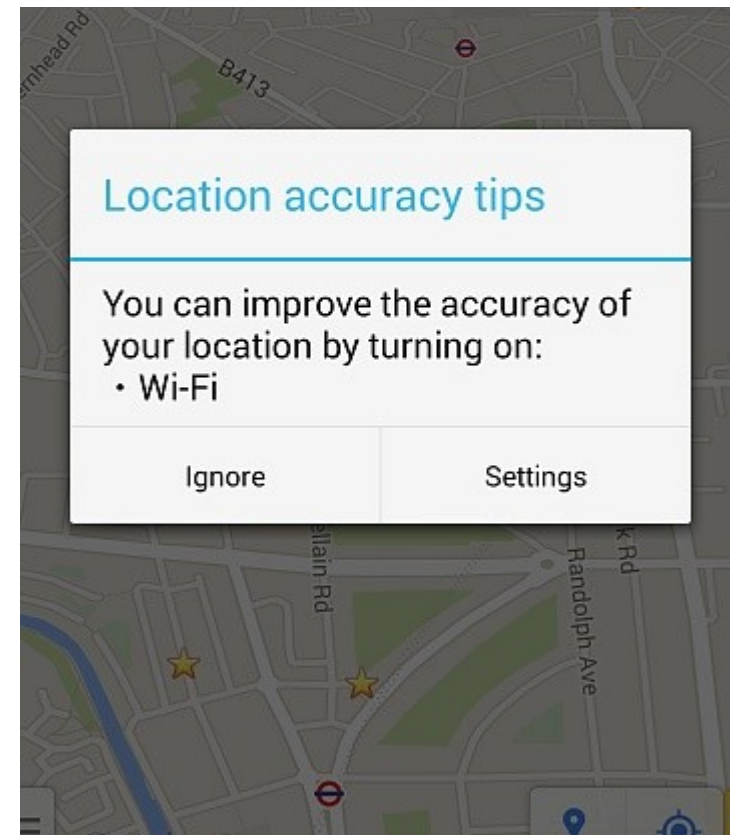


- **June 2016 – labs.integrity.pt – Bug bounty write up**
- **Bugs in Uber app:**
 - waybill feature allowing to retrieve previous users trip details when calling a driver
 - Users enumeration with full details (location of course) using phone numbers

Wi-Fi SSID Google Maps



- **2011 – Google SSID tracking drama**
- **Google Maps used nearby WiFi access points SSID to determine your location**
 - To refine precision
 - If you lose GPS signal for a while
- **You can do a similar app of your own using open databases:**
 - <https://www.wigle.net>
- **Or check other community projects:**
 - <https://github.com/sensepost/Snoopy>



Facebook location recommendations



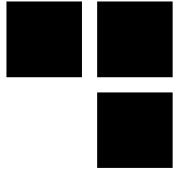
■ June 2016

[-] crimesofthemind 90 points 15 hours ago

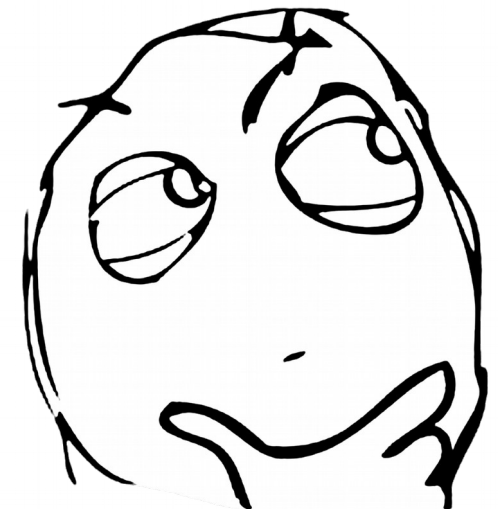
My Facebook app on my iPhone suggested I friend a person who turned out to be the receptionist at my psychiatrist's office, where I had only been once or twice. Really fucking creepy.

I hadn't posted from or (god forbid) checked in at the office. I had only checked/read the news feed while waiting.

- **“we’re not using location data**, such as device location and location information you add to your profile, **to suggest people you may know”**
- **“We often suggest people you may know based on things you have in common, like mutual friends, places you’ve visited [...]. That’s why location is only one of the factors we use to suggest people you may know.”**



Let's think out of the box... with a dating app



Context



- Once upon a time... we looked for love (separately) ... on dating apps of course :-)
- We tested over 9000 apps at least... but not a single real match, bots everywhere :'-(
- We started focusing on GPS-based apps to push our luck a bit!
- How precise is it? Could we follow someone? Let's find out!

Scenario

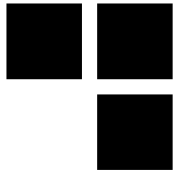


- **Let's say we are women... Everytime we try to find love using mobile apps:**
 - we're spammed by weirdos (here is Jean-Pierre):

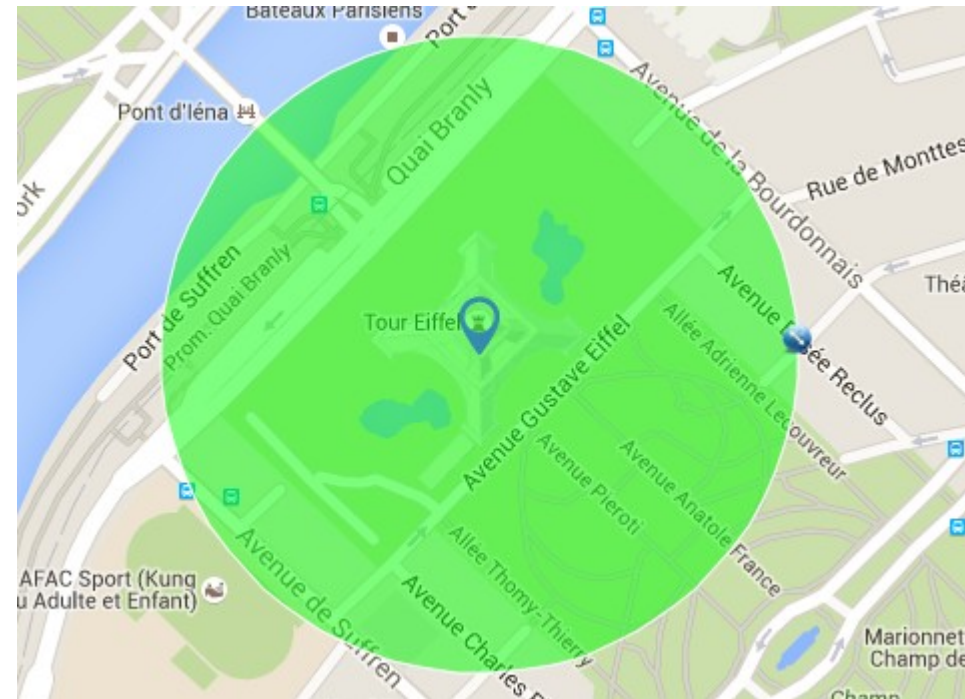


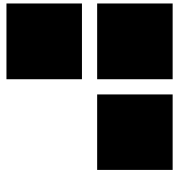
*Ingrid would you f... with me ?

How our targeted app works?



- The app we chose notifies you when you cross people's way
- You are notified only if match preferences are mutual

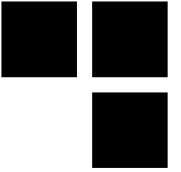




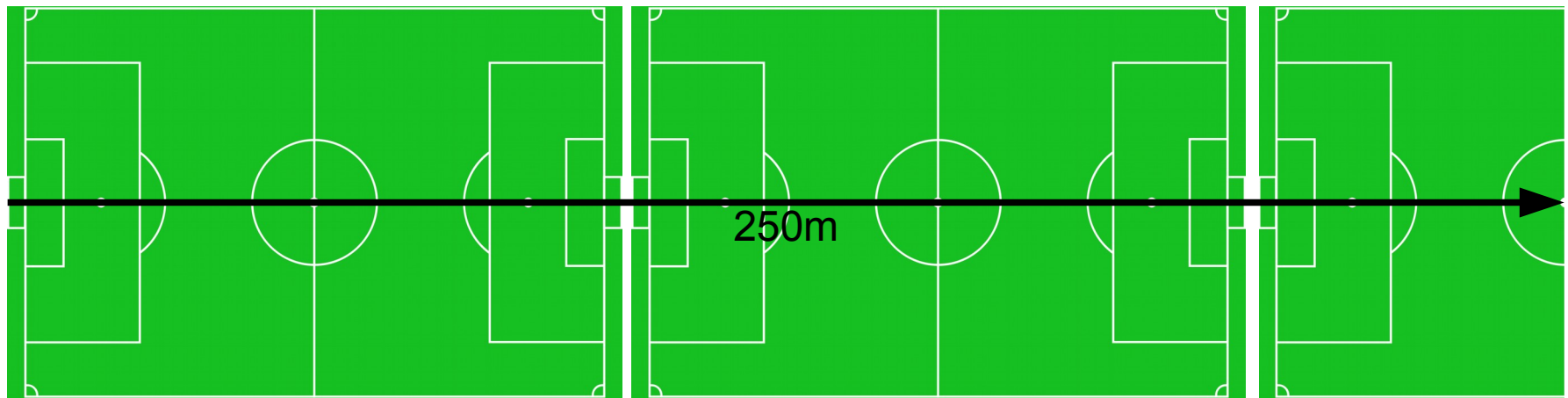
How our targeted app works?

- **The app sends your location to a server all day long**
- **The server computes "matches" regarding location and match preferences**
- **When the server finds a match:**
 - It tells you where and when you were when you crossed someone's path
 - It tells an approximative distance limited to these values:
250m, 500m, 750m, 1km

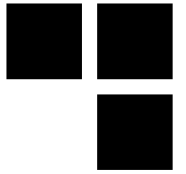
First problems



- Precision ...

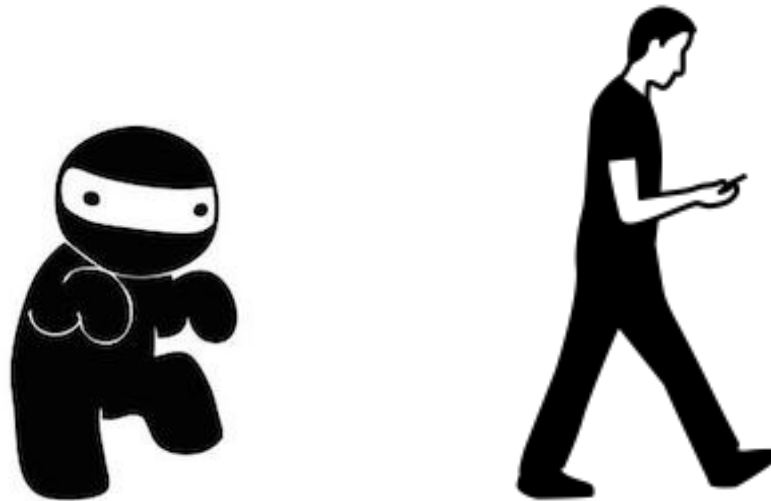


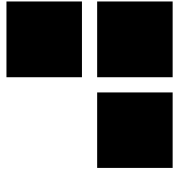
- Wow! That's far! (and 360°!)
- **If you move too fast, the server sets a timeout before you can update your location (5 minutes)**



Goals of this talk

- **Improve the precision so we can catch Jean-Pierre!**
- **Be able to follow him for a while**

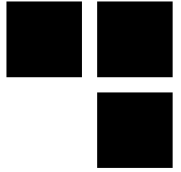




But, how does geolocation work

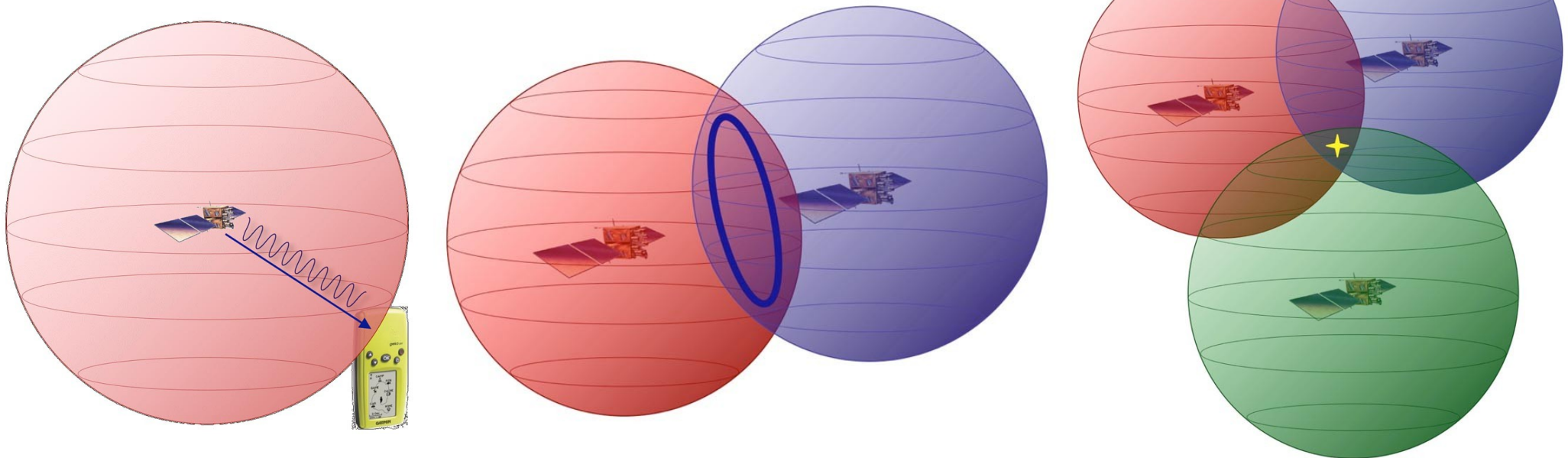


But... How to geoloc? 101



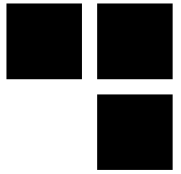
■ Satellites (GPS)

- 3 satellites needed to get an approximation



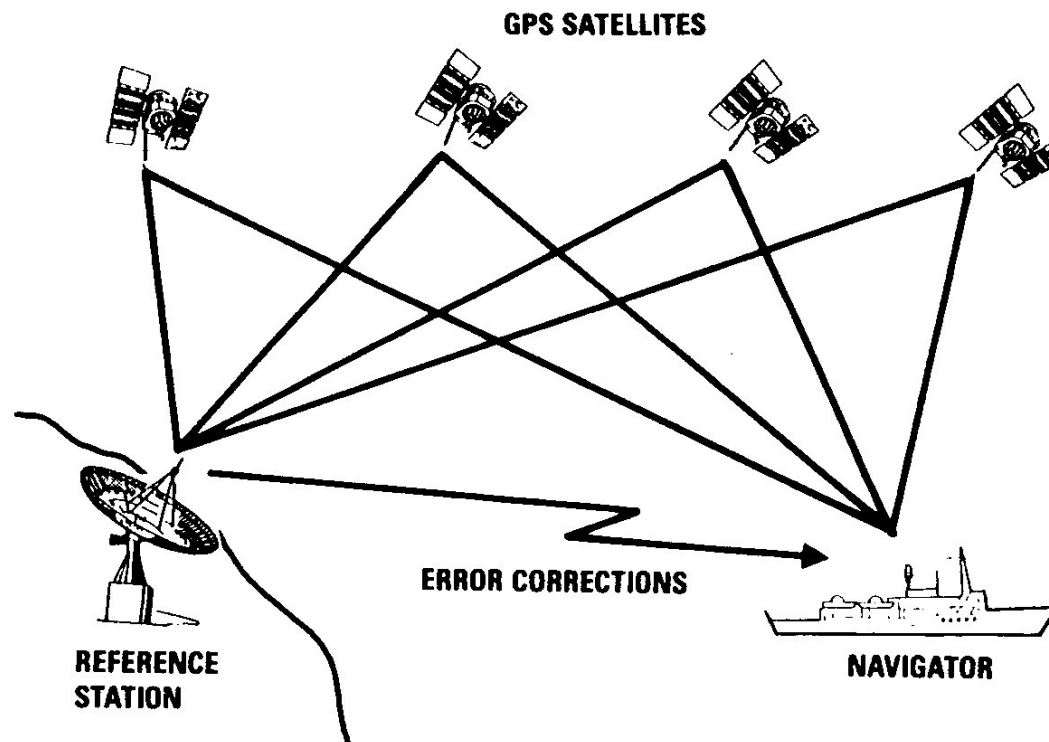
- In practice, it uses between 4 and 12 satellites to get a precise location
- 3-8m precision for civilian use, 1-3m for military use

But... How to geoloc? 101



■ Differential GPS (DGPS)

- Same approach but adds a terrestrial fixed point
- Few centimeters precision after post-treatment





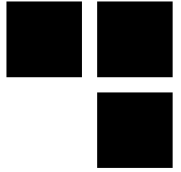
But... How to geoloc? 101

■ GSM geolocation

- Most used technique: Cell ID
- Determine the position based on which antennas are in range
- Can be used by users themselves to navigate:

<http://opencellid.org/>

What do we need...



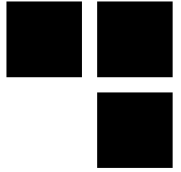
- **To refine Jean-Pierre's location?**
 - Bring friends! They will be our satellites!
- **To track efficiently and avoid being spotted?**
 - Bring even more friends!



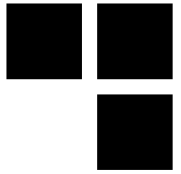


OK! Let's bring up friends!

The devil is in the details



- **Preferences match**
- → **All our agents must respond to the same characteristics.**
 - 30 y/o women looking for men (and women if you want to extend)



What is an agent?

- **No need to get a phone by agent (too expensive)**
- **Intercepts the HTTP requests sent by the app**
- **Only 3 types of interesting requests:**
 - Login via Facebook
 - Update my current location
 - Who is around me?
- **Replay these 3 requests to simulate a regular user with a few lines of python**



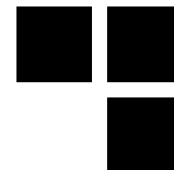
Problems start...



- **The app requires a Facebook account to authenticate**
- **Somehow, Facebook thinks we're creating bots... nasty little Facebook!**



Facebook suspicion



- Facebook sometimes asks you for an ID card or a phone number

Please complete a security check

Security checks help keep Facebook trustworthy and free of spam.

Use a phone to verify your account

The phone number you use can only verify one account. Once you enter your number, you'll receive a code that you'll be able to enter on Facebook to verify your account. Your phone number will only be used to verify your account and will not be shared with anyone without your consent.

[Enter a phone number](#)

[I need help.](#)

[Continue](#)

Upload Your Photo ID

To make sure this is your account, we need you to upload a color photo of your government-issued ID. Your ID should include your name, birthday and photo.

Acceptable IDs include your:

- Passport
- Driver's license
- State-issued ID card
- Military ID card
- Immigration ID with signature

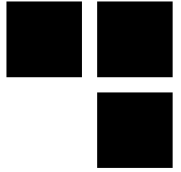
Please keep in mind that we can't accept your profile picture.

Once we receive and review a clear image of your ID, we will permanently delete your attached identification document from our servers.

[I don't have a government-issued ID](#)

[Continue](#)

Solutions



■ FREE!

- Ask real friends to receive the confirmation code (annoying)
- ~~Online SMS services~~: All phone numbers are blacklisted or already in use

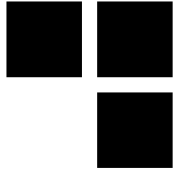
■ \$

- Get an alternative number from your operator

■ \$\$\$

- Buy several Facebook accounts from an East European shop



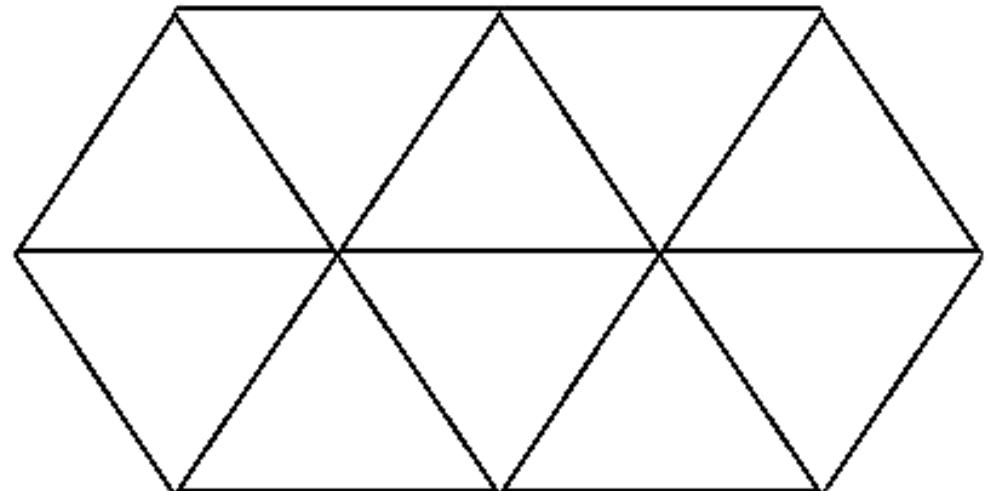
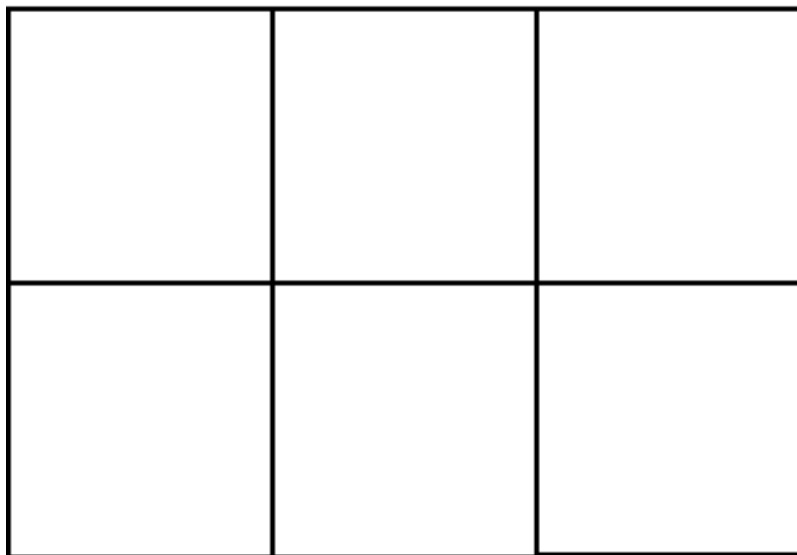


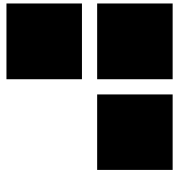
Now we have agents,
how to place them efficiently?



Dispatch agents

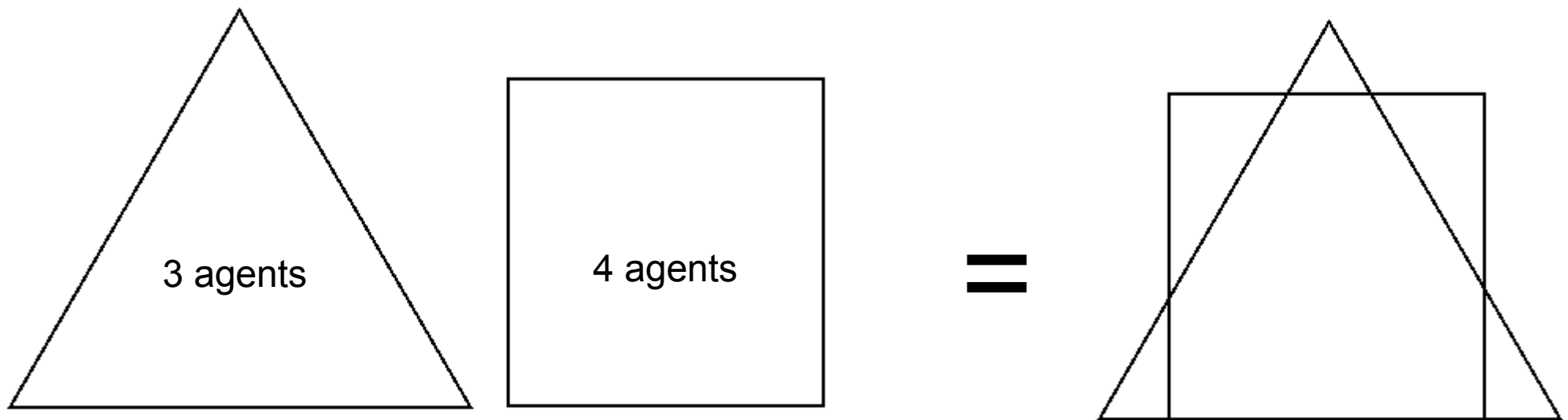
- Limited number of agents
- How to optimize the space covering?
- And keep satisfying location results
- Tessellation, Tiling





Dispatch agents

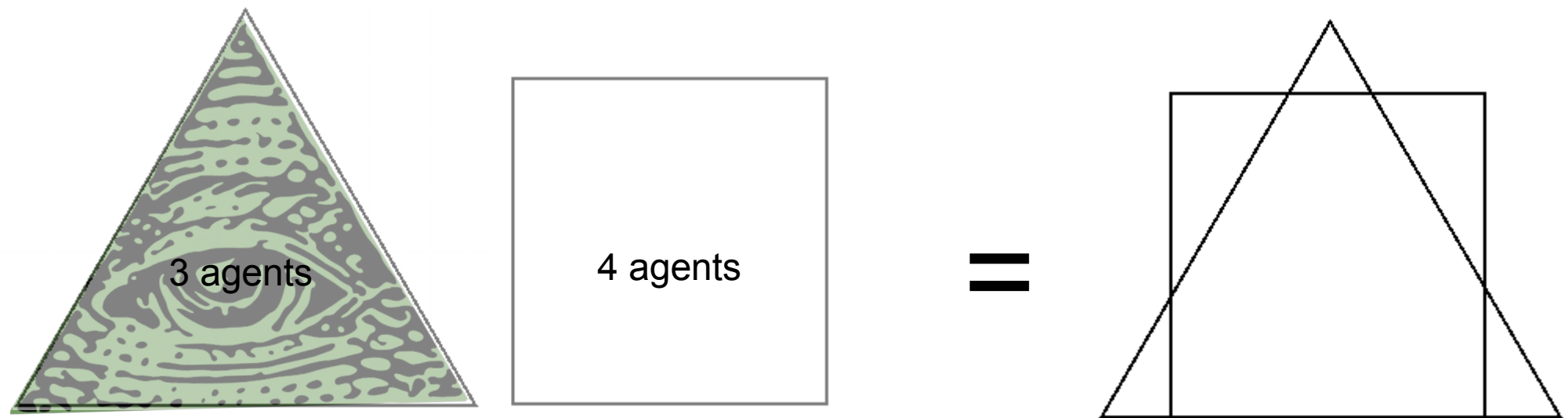
- **Square or triangles?**
 - Same area



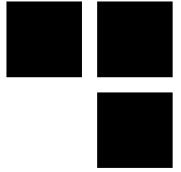


Dispatch agents

- **Square or triangles?**
 - Same area

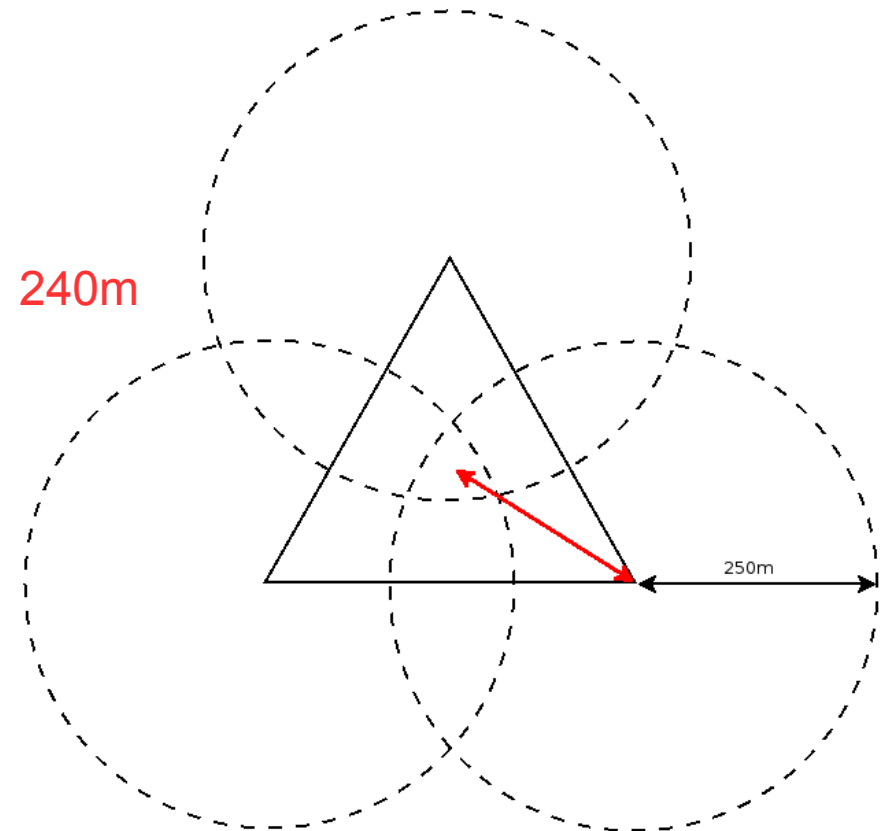
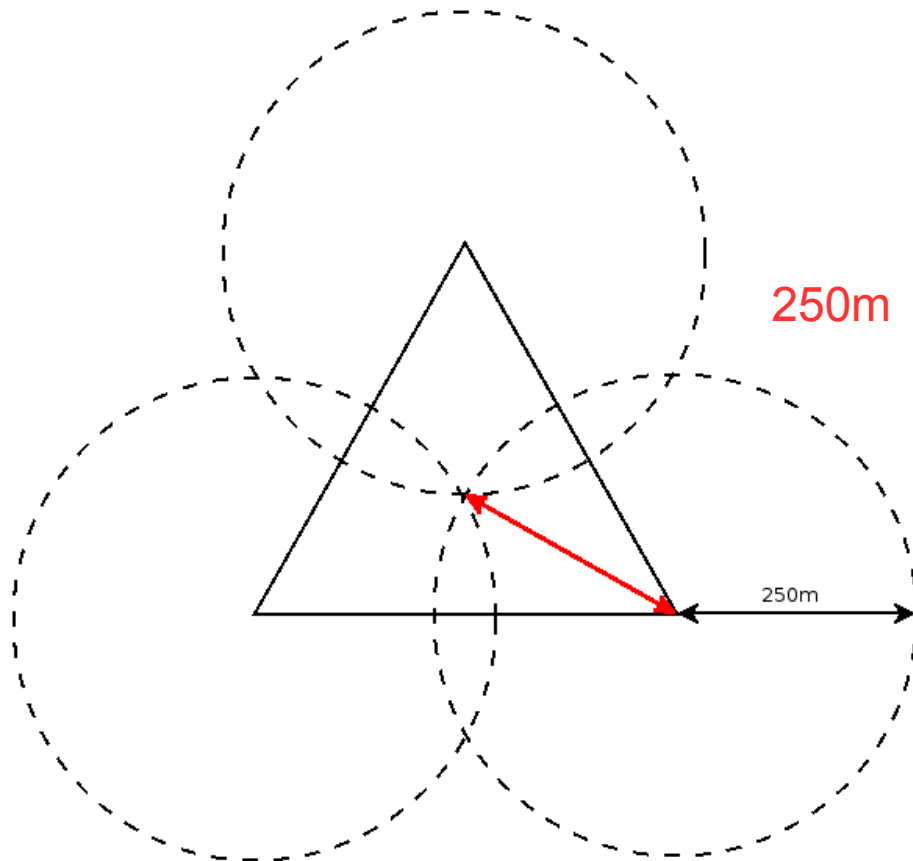


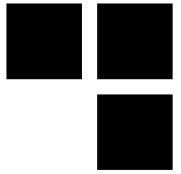
Dispatch agents



- **Ok we chose triangles**

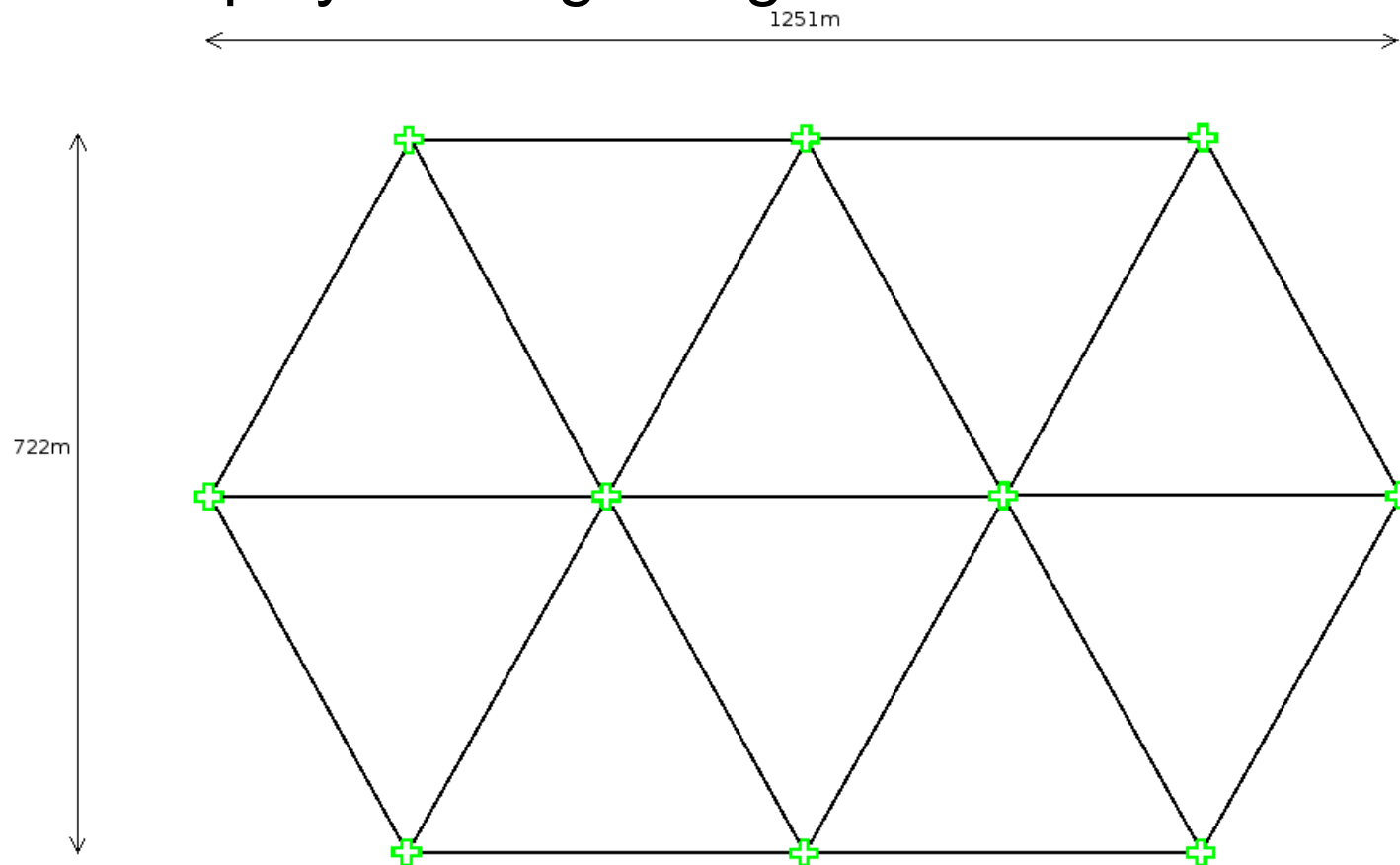
- Now: How to space our agents?

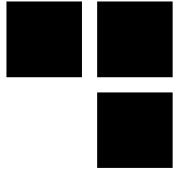




Tiling with triangles

- **240 meters seems good**
 - Let's deploy a 10 agents grid

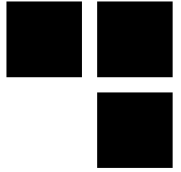




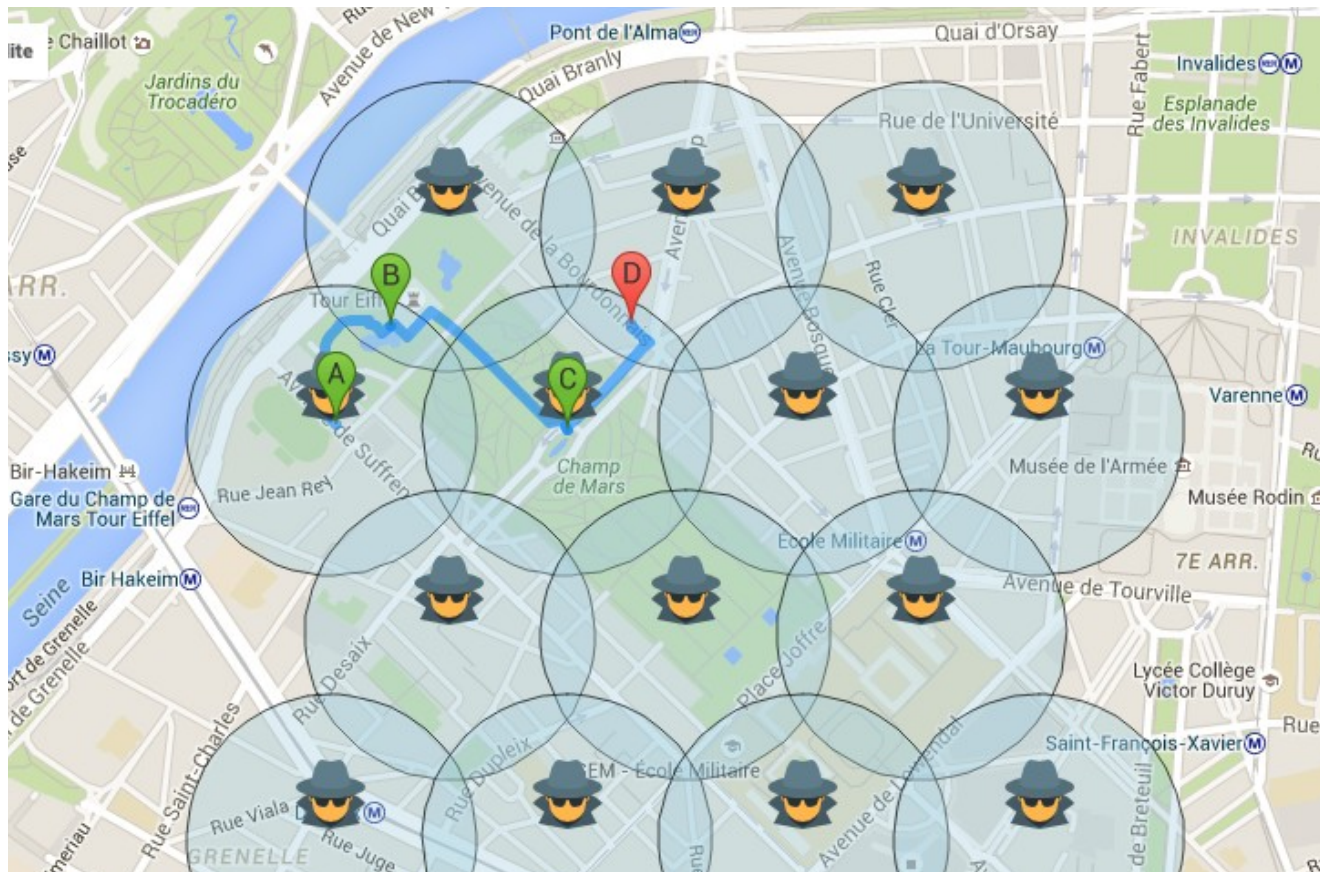
A few stats

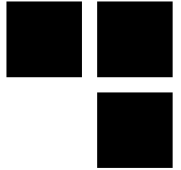
- **Number of agents needed to cover:**
 - Disneyland Paris: ~75 agents
 - Paris: ~1K agents
 - France: ~ 6M agents

We are legion ...



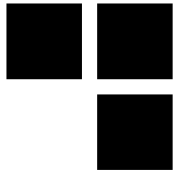
- Same view on a real map





Jean-Pierre enters our (in)grid!

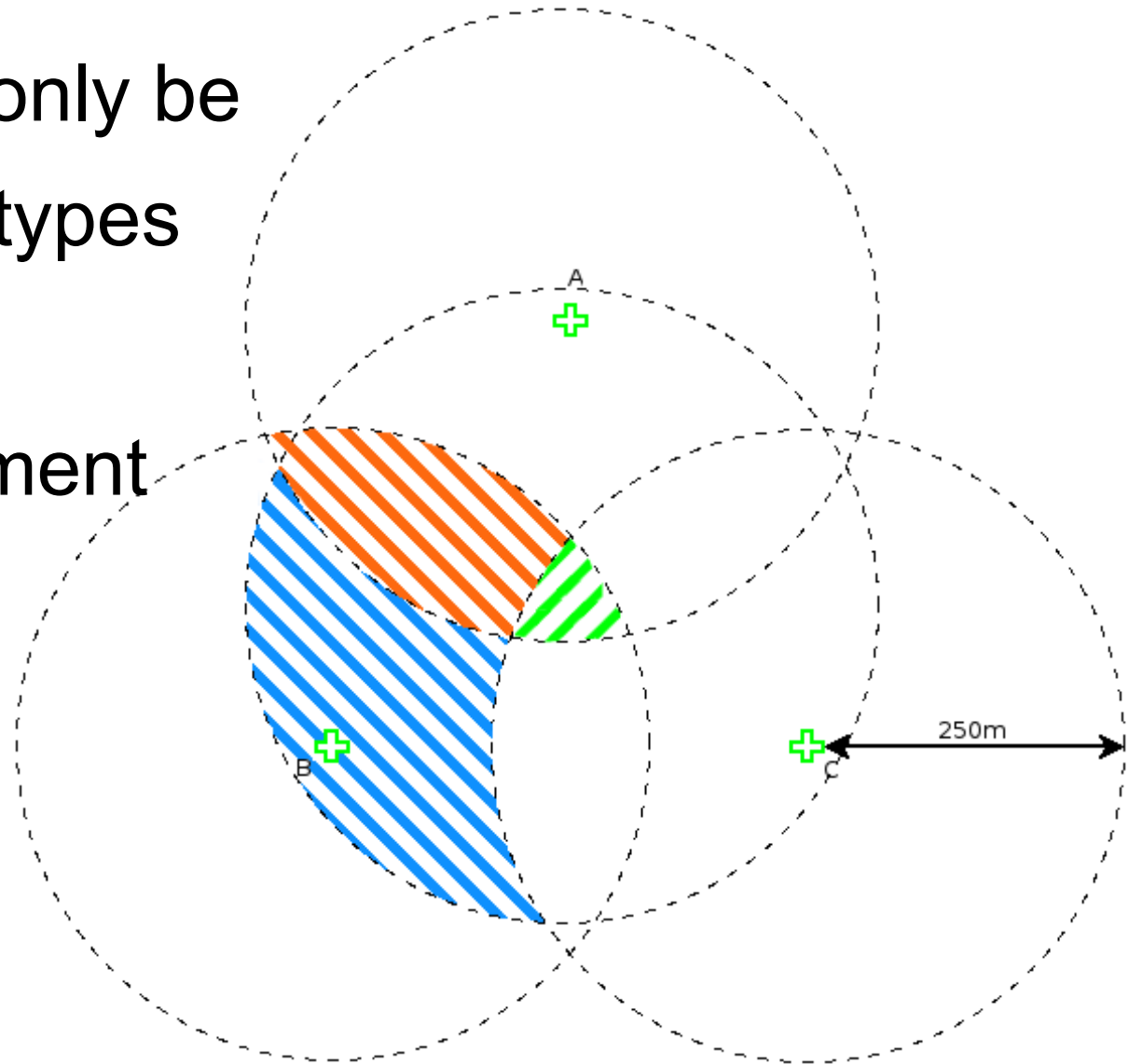
Precision improvement



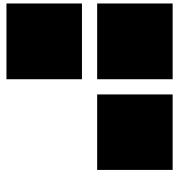
- Jean-Pierre could only be located in 3 different types of area

- Precision improvement

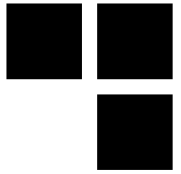
- Blue : x 4
- Orange : x 18
- Green : x 357



Can't we do better?

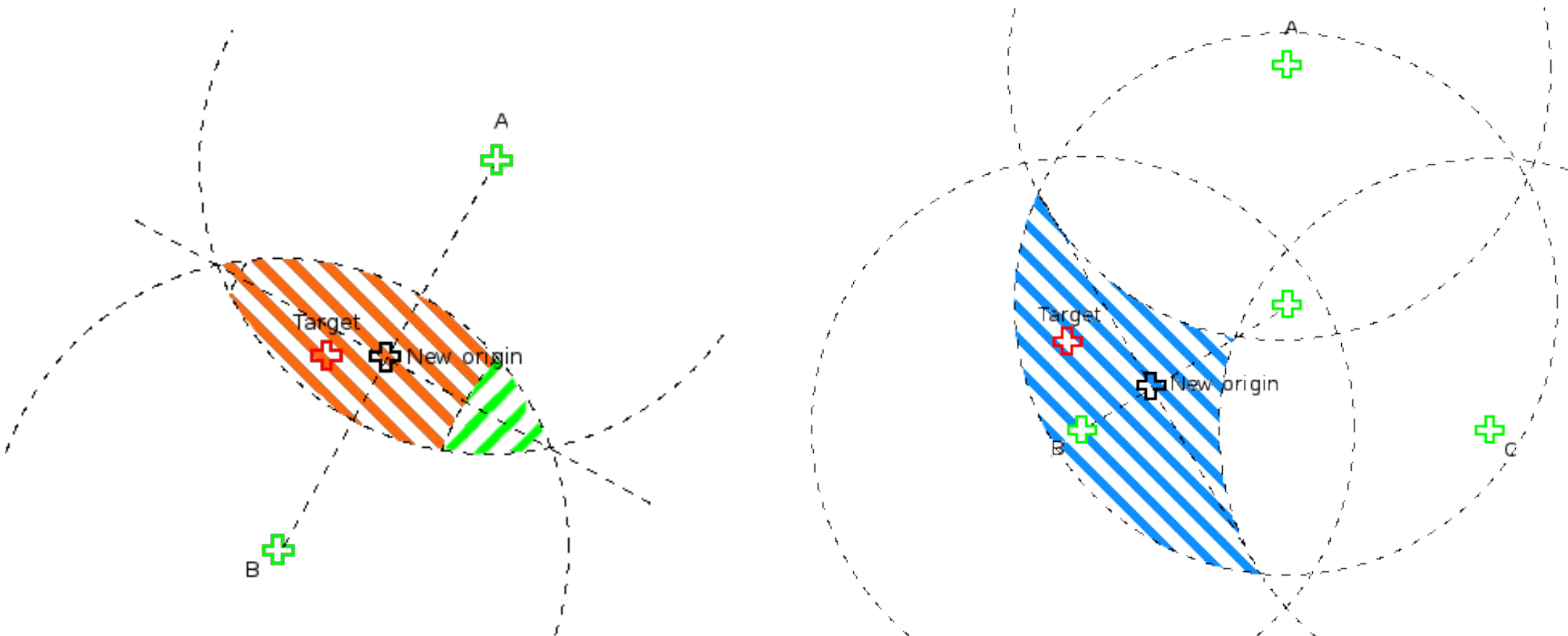


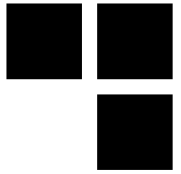
- **Blue** and **Orange** cases are more precise but still not satisfying
- What if we move our agents and try to get Jean-Pierre in the **Green** zone?
 - Reminder: Our agents just moved and there might be a 5 minutes timeout before they can move again
 - Solution: Recruit 3 flying agents!



How to build a 6 pack?

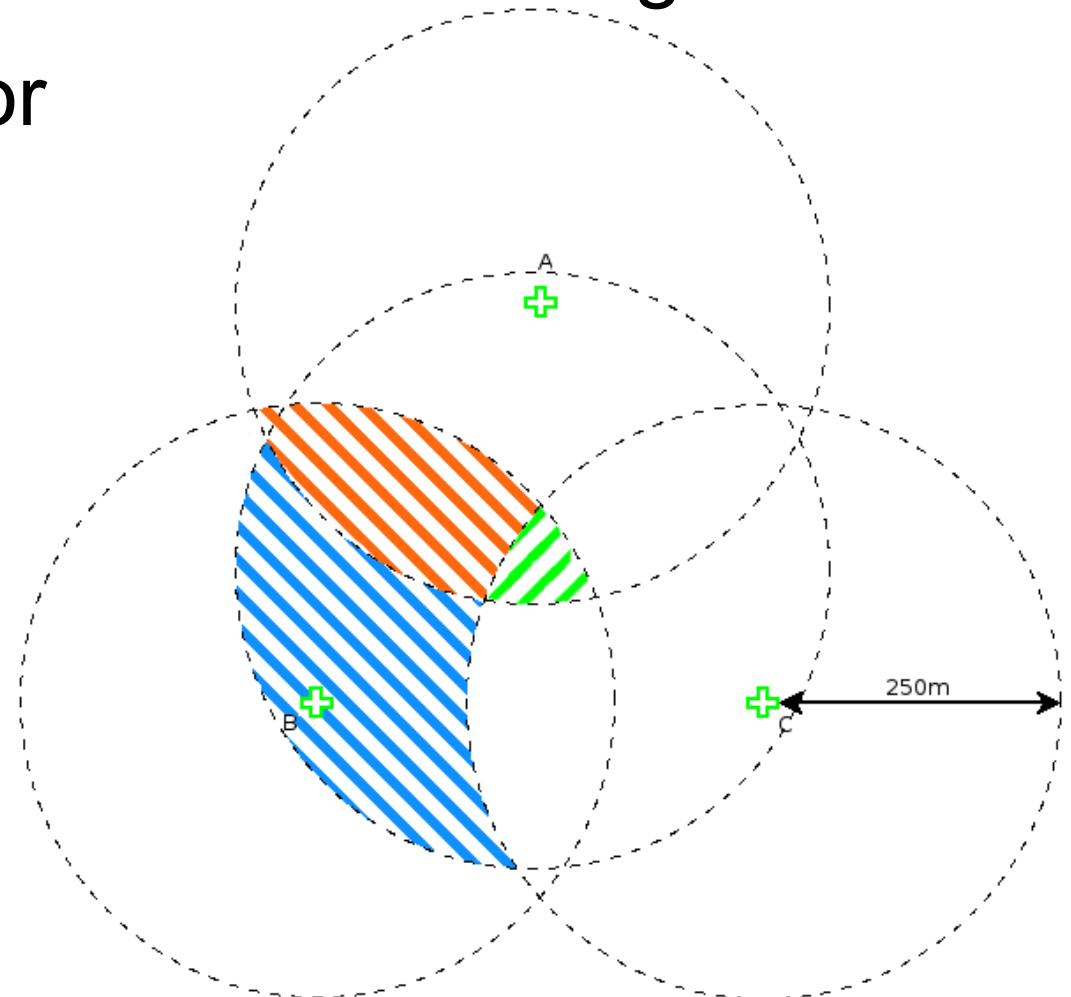
- Define a new origin
- Refine **Orange** and **Blue** cases!





Precision improvement 2

- Repeat the process from the new origin
- 6 agents required for the operation

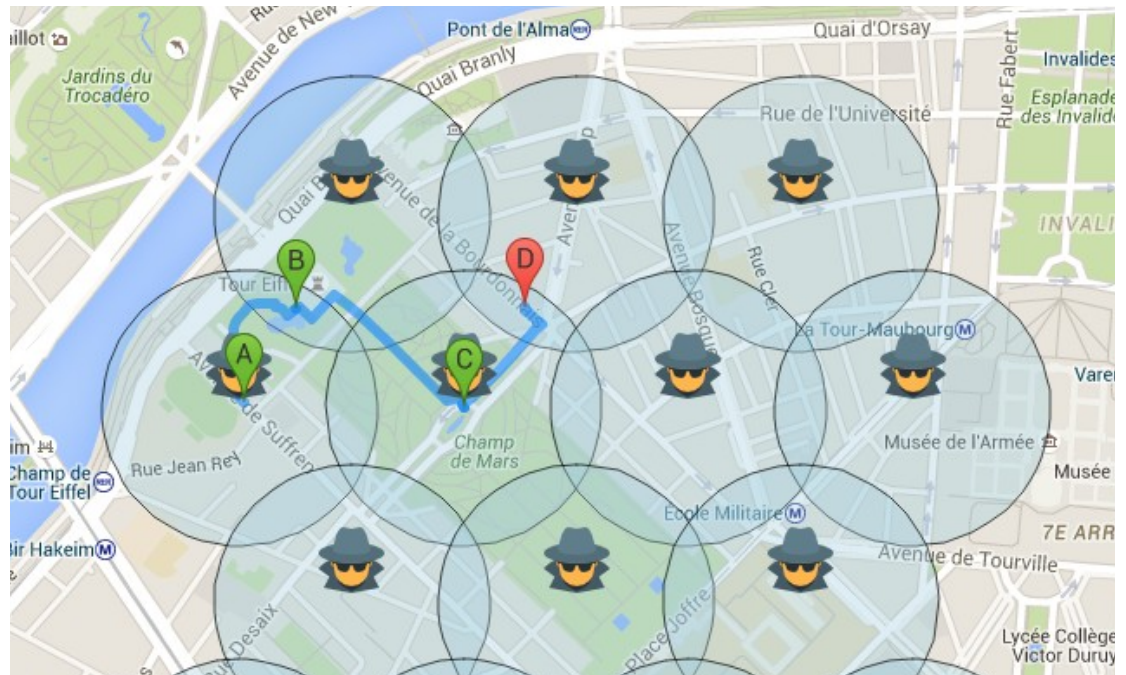




Let's put all that geometry stuff inside a web app

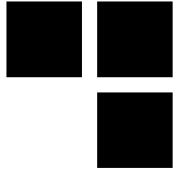
Idle mode

- Deploy the grid
- List potential Jean-Pierres detected by friends
- Monitor people's moves



Track mode


- Jean-Pierre is in the grid!
- Improve precision
- Shift the grid to keep him in the center
- Repeat





It works!


- 2017 trends: Python, Flask, Bootstrap, Docker, Google Maps API ...


Where is Jean-Pierre? [Users](#) [Targets](#)


 **Jean-Pierre 117** (age: 26, history: 5) - Last seen : 17 June 2016 13:57
ID: 117, Facebook ID: 100012445182757 >


 **Jean-Pierre 265** (age: 53, history: 5) - Last seen : 17 June 2016 14:49
ID: 265, Facebook ID: 100012445182757 >


 **Jean-Pierre 93** (age: 34, history: 4) - Last seen : 16 June 2016 19:00
ID: 93, Facebook ID: 100012445182757 >

 **Jean-Pierre 230** (age: 27, history: 4) - Last seen : 17 June 2016 14:52
ID: 230, Facebook ID: 100012445182757 >

 **Jean-Pierre 235** (age: 40, history: 4) - Last seen : 17 June 2016 14:31
ID: 235, Facebook ID: 100012445182757 >


 **Jean-Pierre 282** (age: 30, history: 4) - Last seen : 17 June 2016 14:16
ID: 282, Facebook ID: 100012445182757 >

 **Jean-Pierre 300** (age: 24, history: 4) - Last seen : 17 June 2016 14:46
ID: 300, Facebook ID: 100012445182757 >

 **Jean-Pierre 27** (age: 27, history: 3) - Last seen : 17 June 2016 14:26 >

Position history of Jean-Pierre 93 [See Facebook profile](#) [Set as target](#)

Date	Lon	Lat
16 June 2016 18:46	2.292559	48.856350078
16 June 2016 18:48	2.29394767173	48.857932539
16 June 2016 18:58	2.29811368694	48.856350078
16 June 2016 19:00	2.29950235867	48.857932539

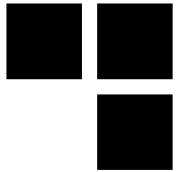






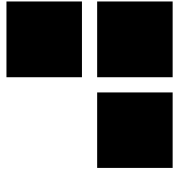
Mitigations

- **Possibility to turn on invisible mode**
 - Similar as a plane mode
 - Used by other similar apps to protect users
- **Possibility to blacklist some users**
 - If you don't like them
 - If you feel they might be following you
 - Whatever reason



Extending the tool

- **Detect if an agent have been blacklisted by Jean-Pierre**
- **Use other geoloc methods as "plugins"**
- **Intersect data sources to improve precision**
- **Crawl related social networks to find more location data**
 - Google+ images EXIF data
 - Facebook Nearby friends or location pinning



Conclusion

- **Now we are able to**
 - locate Jean-Pierre quite precisely
 - track him for a while
- **Almost any app using GPS can be turned into a tracking system, we just need:**
 - A user identifier
 - Partial location
 - Timestamp
- **You don't need to be a government agency or an Internet Giant to do it!**

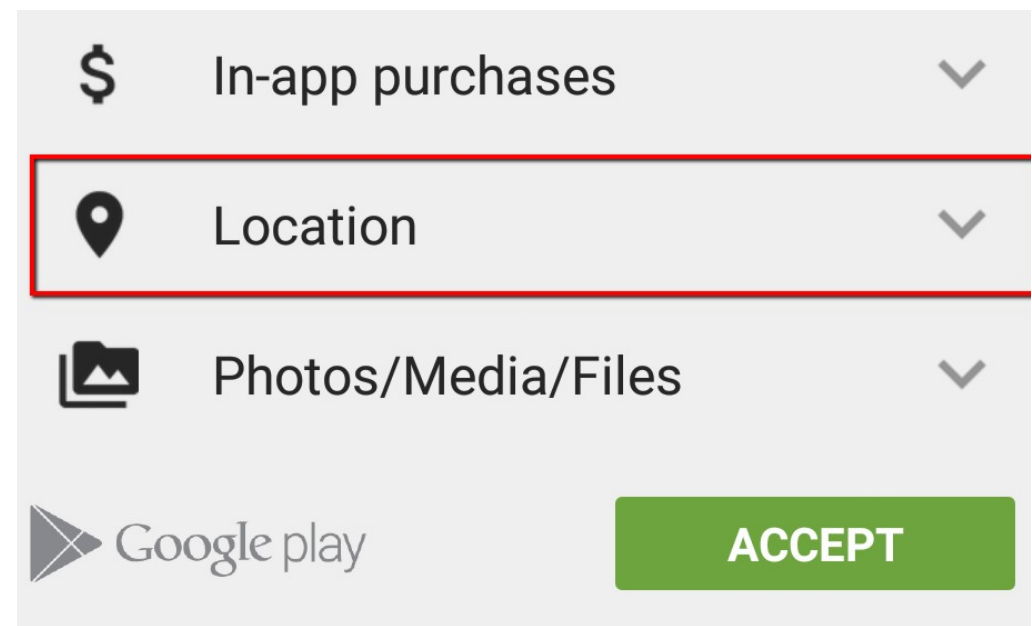


Conclusion

■ When installing an App

- Try to think how it could be used against yourself
- Not limited to location (WiFi, Bluetooth, NFC...)

■ Don't be a Jean-Pierre





ANY QUESTIONS?



Thank you for your attention!

