RECHERCHE

INSTITUT NATIONAL DES SCIENCES APPLIQUEES DE LYON

Device-to-Identity linking attack using targeted Wi-Fi geolocation spoofing

Célestin Matte - Jagdish Achara - Mathieu Cunche

ACM WiSec 2015

Outline of the talk

1 Introduction

2 Background

3 Description of the attack

4 Tests and results

5 Conclusion

Introduction

- Mobile devices are trackable because they emit probe requests [2]
- But only through an "anonymous" identifier: the MAC address
- Is it *really* anonymous?
- Problem: *given a mobile device identified by a Wi-Fi MAC address, find the identity of the owner of this device.*
- Solution: attack on Wi-Fi-based Positioning Systems (WPS)
- Outcome: get personal information: identity of the device's owner $\rightarrow$ account on geotagged services (example with Twitter)

Background

- Wi-Fi service discovery
- Wi-Fi based geolocation
- Spoofing geolocation

- How do devices know which Wi-Fi access points (APs) are present?
- Two methods:
  - passive discovery: APs broadcast beacons
  - active discovery: devices send probe requests (with or without SSIDs), APs respond with probe responses

- One geolocation method uses visible access points to locate devices
- Mainly used when GPS is not available or not available yet (i.e., inside building), or to save battery

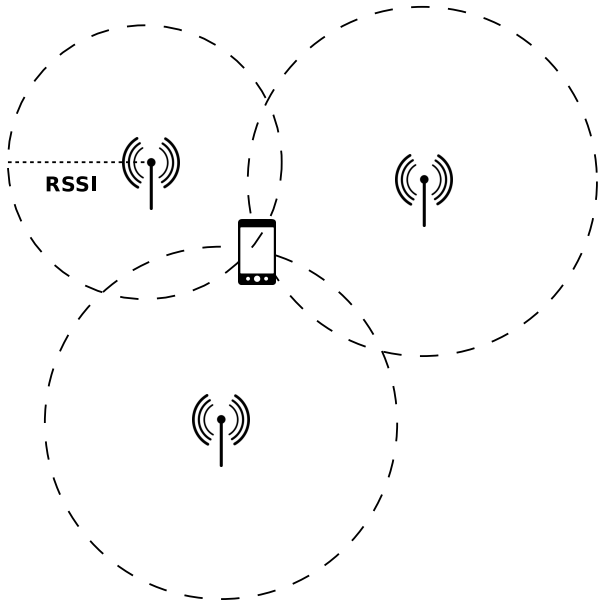
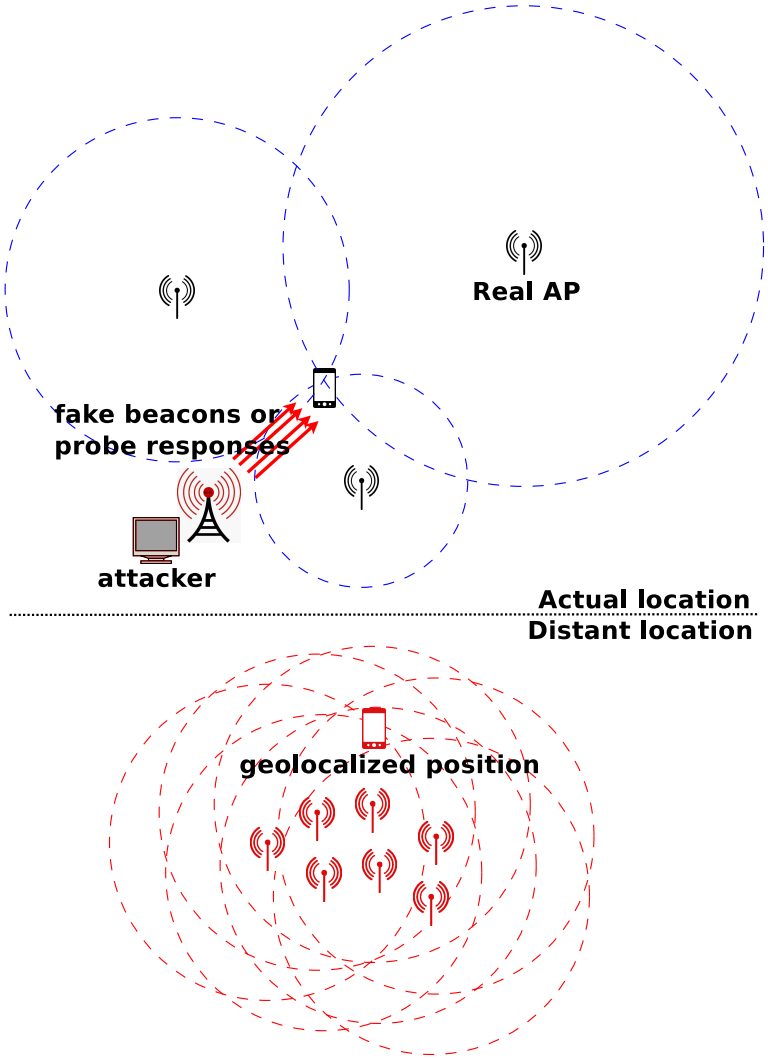


Figure: Geolocation via trilateration based on visible Wi-Fi access points.

Based on a previous work [3]



Description of the attack

- Targeted spoofing
- Description
- Testing WPS
- Implementation

Targeted spoofing

- Problem: original attack supposes that there is only one device in range. What if we want to target only one device among other ones?
- Passive discovery:
  - Beacons are broadcast (destination address = ff:ff:ff:ff:ff:ff)
  - Can it simply work without broadcast? (targeted destination address)
- Active discovery:
  - simply reply to broadcast probe requests from only one device

Targeted spoofing

- Problem: original attack supposes that there is only one device in range. What if we want to target only one device among other ones?
- Passive discovery:
  - Beacons are broadcast (destination address = ff:ff:ff:ff:ff:ff)
  - Can it simply work without broadcast? (targeted destination address)
    - Yes.
- Active discovery:
  - simply reply to broadcast probe requests from only one device

Attacker model

- Two kind attackers:
  - simple: physically close to the target, can only access public information
  - powerful: also close to the target, but can access private information (no need to be “friend” with the target)

Description of the attack

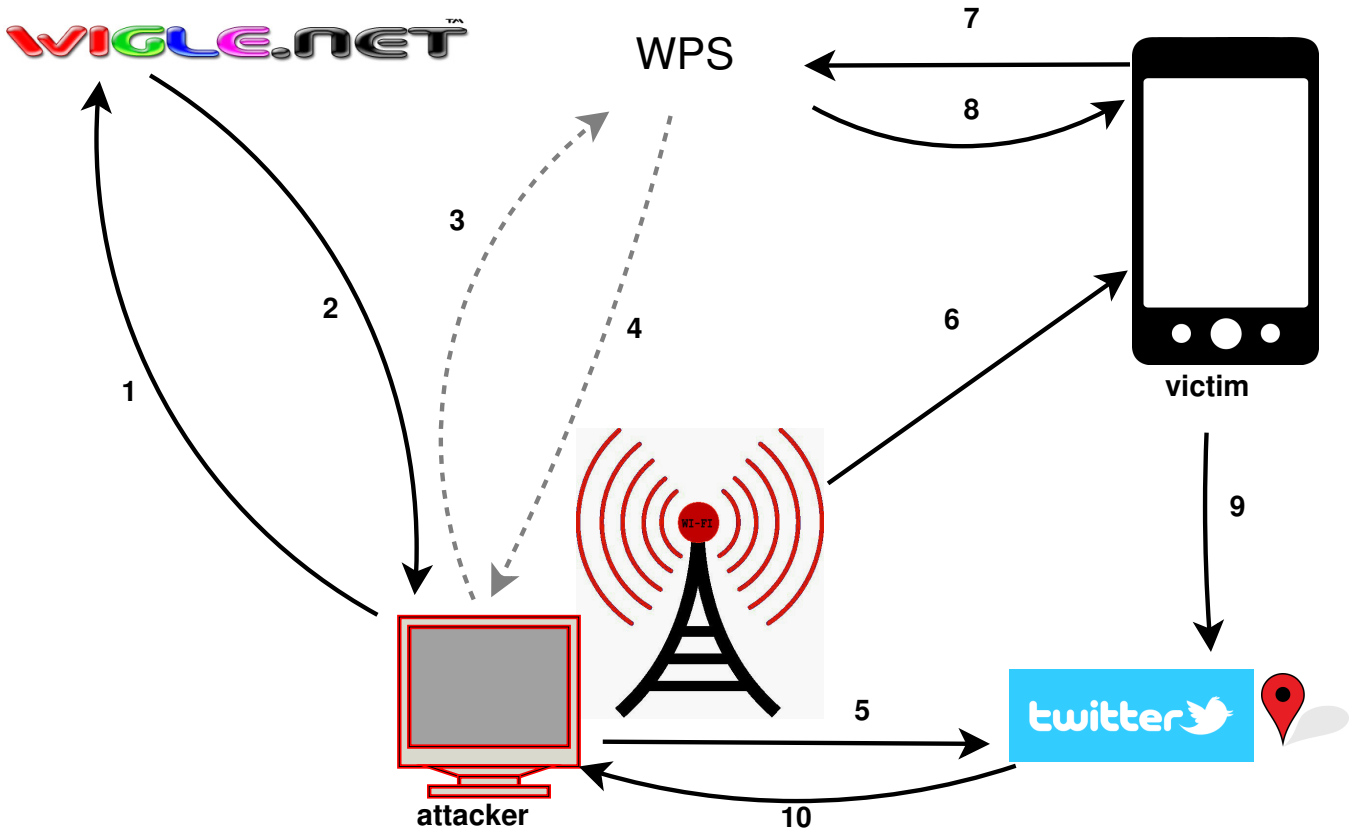


Figure: Description of the attack (dotted lines: optional)

- Testing geolocation spoofing on WPS
- Implementation
- Results - Example
- Results - discussion
- Testing the attack on different Android apps

Testing geolocation spoofing on WPS

- Can we avoid jamming? How do WPS react if we send AP from different locations?
- Evaluation on multiple WPS: GoogleGeoloc, Navizon, Skyhook
- Navizon takes history into account

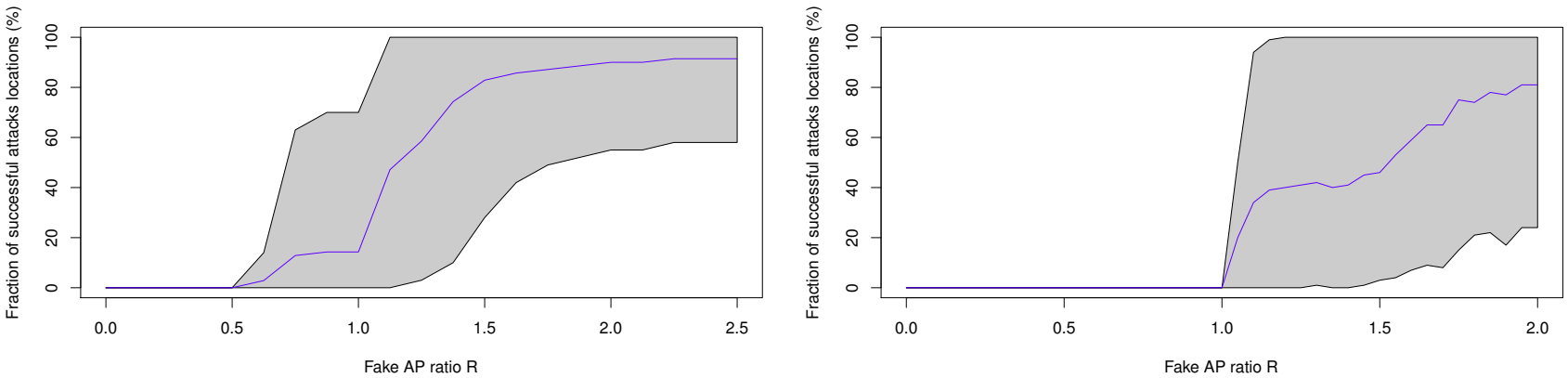


Figure: Fraction of successful attacks: number of AP from original location over number of AP from destination location (left: Google geolocation API; right: Skyhook)

Implementation

- Some bash + perl + php scripts
- Does everything automatically
- Available on github [1]

Results - example

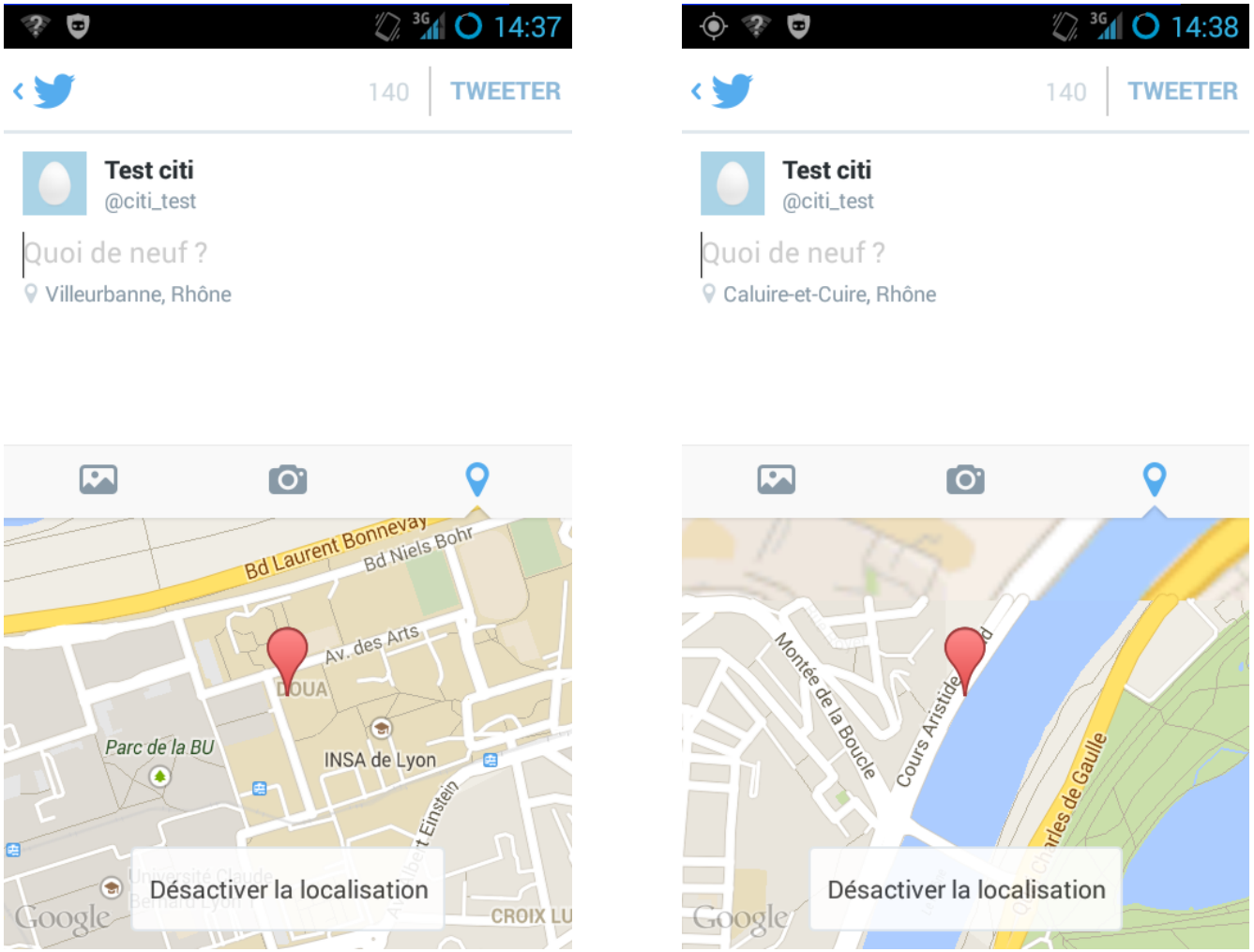


Figure: The Twitter application, before and during the attack.

- Tested on Android and iOS
- Never worked on iOS
- No need to jam legitimate APs
  - ...But: does not always work, mainly depending on the number of real access points, and the distance of the fake location

Testing the attack on different Android apps

Application name	public geolocation	Result of geolocation spoofing	
		GPS off	GPS turned on, then off
Messenger (Facebook)	✗	✗	✗
Facebook	✗	✓	✗
Twitter	✓	✓	✓
Google+	✓	✓	✓
Foursquare	✓	✓	✗
Swarm	✗	✓	✗
Instagram	✓	✗	✗
Tinder	✓	✓	✓
Badoo	✓	✓	✓
LOVOO	✓	✓	✓
RunKeeper	✗	✗	✗
Nike+ Running	✗	✗	✗
Waze	✓	✗	✗
Glympse	✓	✓	✓
Glympse Express	✓	✓**	✓**
Runtastic	✗	✓	✓

**: only if the attack is launched beforehand

Figure: Result of the Wi-Fi geolocation spoofing on selected Android applications

Conclusion

- Attack on Wi-Fi-based positioning systems
  - Contributions: jamming not necessary, targeted attack $\rightarrow$ allow full attack
- Generate a fake Wi-Fi environment
- Get user information: account name on applications publishing location
- Evaluated the attack on various WPS and Android apps

Bibliography


Public repository of the test script.
`https://github.com/Perdu/geoloc_attack`, consulted on 2014.04.07.


M. Cunche, M. A. Kaafar, and R. Boreli.
I know who you will meet this evening! linking wireless devices using wi-fi probe requests.
In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, pages 1–9. IEEE, 2012.


N. O. Tippenhauer, K. B. Rasmussen, C. Pöpper, and S. Čapkun.
Attacks on public wlan-based positioning systems.
In *Proceedings of the 7th international conference on Mobile systems, applications, and services*, pages 29–40. ACM, 2009.