Lesson 10 – Privacy concerns regarding geolocation

Introduction

This lesson focuses on privacy risks caused by usage of geolocation features in the application and that may allow a malicious third party to get the location of the victim.

Trilateration is the process of determining the location of points by measurements of distances. This term is often used interchangeably with triangulation, but triangulations uses angle measurements instead of distances. It could be used in applications that show distance to a user in order to find out the exact position of this user.

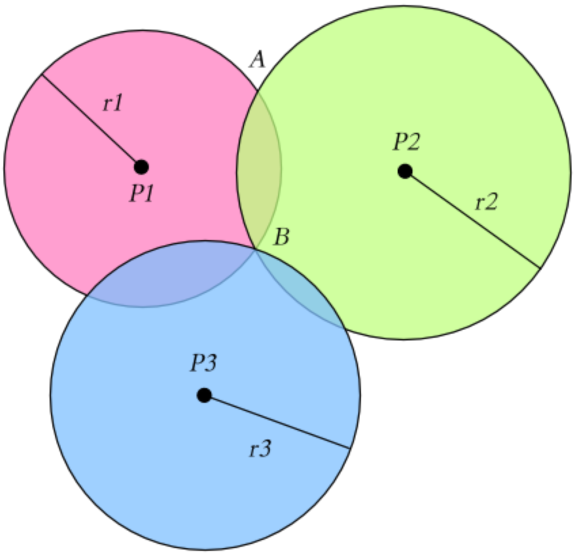


Illustration 1: Example of trilateration.
Source: Wikipedia

Getting started

You will need:

- an Android device or an emulator,
- a desktop with intercepting proxy.

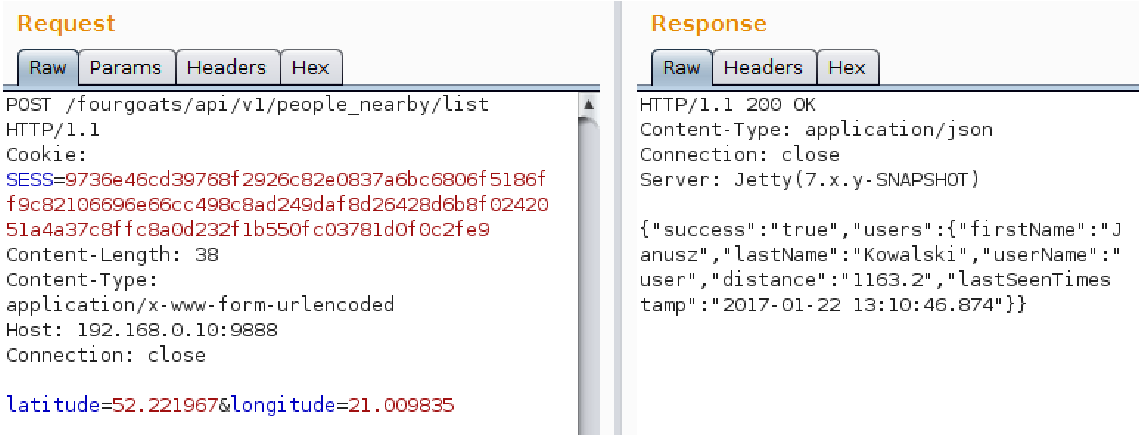
The setup is the same as in the Insecure Communication lesson.

Finding vulnerabilities

The People Nearby feature shows the distances to People Nearby with an accuracy to 1m. Try to find out more by recording the application traffic with Burp.

The application sends latitude and longitude with a POST request to the server, and gets a JSON response with profile data and their distances to the given location.

Try to use repeater to repeat this packet with different location. You will manage to get different distances. It could be used by an attacker to perform trilateration in order to find the exact location of the victim.



```
POST /fourgoats/api/v1/people_nearby/list
HTTP/1.1
Cookie:
SESS=9736e46cd39768f2926c82e0837a6bc6806f5186f
f9c82106696e66cc498c8ad249daf8d26428d6b8f02420
51a4a37c8ffc8a0d232f1b550fc03781d0f0c2fe9
Content-Length: 38
Content-Type:
application/x-www-form-urlencoded
Host: 192.168.0.10:9888
Connection: close

latitude=52.221967&longitude=21.009835
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Connection: close
Server: Jetty(7.x.y-SNAPSHOT)

{"success":"true","users":{"firstName":"J
anusz","lastName":"Kowalski","userName":"
user","distance":"1163.2","lastSeenTimes
tamp":"2017-01-22 13:10:46.874"}}
```

Illustration 2: Request and response of People Nearby feature

Exploiting vulnerability

Try to send three packets with different locations and get three distances of a user from these locations. For this lesson the locations of Warsaw University of Technology, University of Warsaw and Warsaw Uprising Museum have been chosen. The position of the victim could be determined by using calculations, or just visualized by drawing. The Free Map Tools web page (https://www.freemaptools.com/radius-around-point.htm) have been used for drawing circles of a given radius on the map. This resulted in these circles intersecting at the Palace of Culture – the location of a victim of the attack.

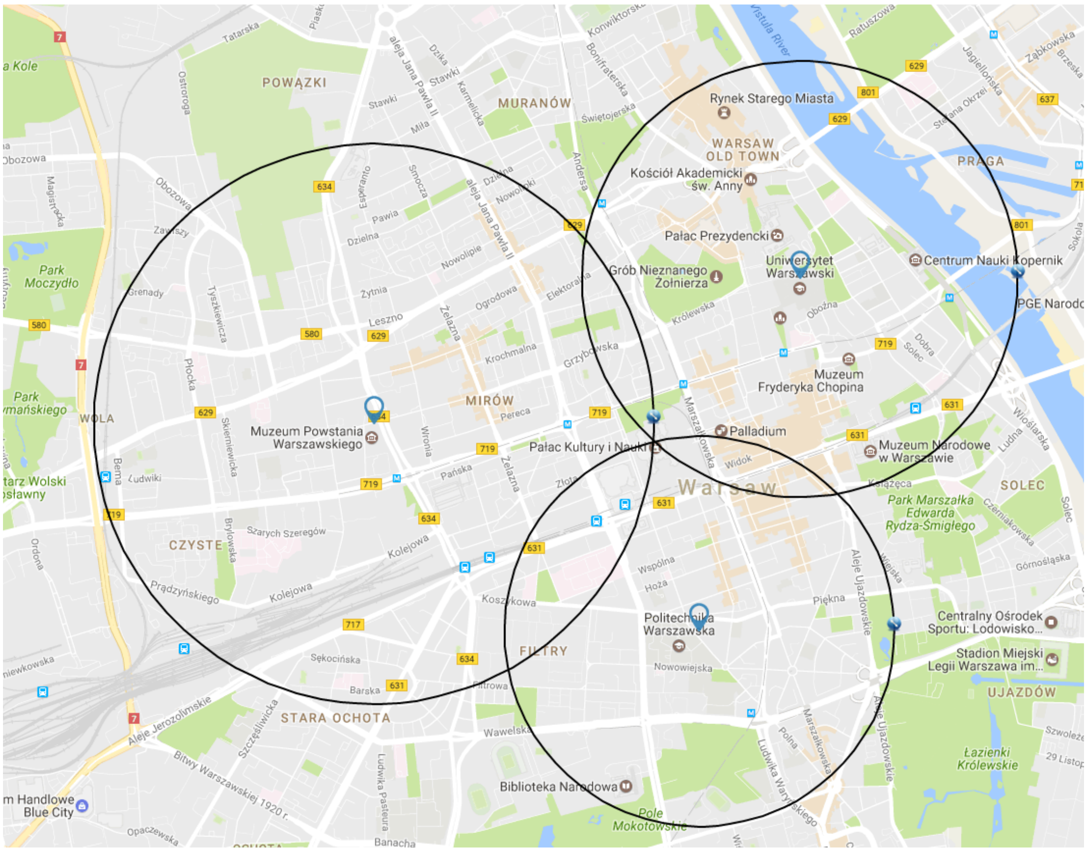


Illustration 3: Effect of trilateration

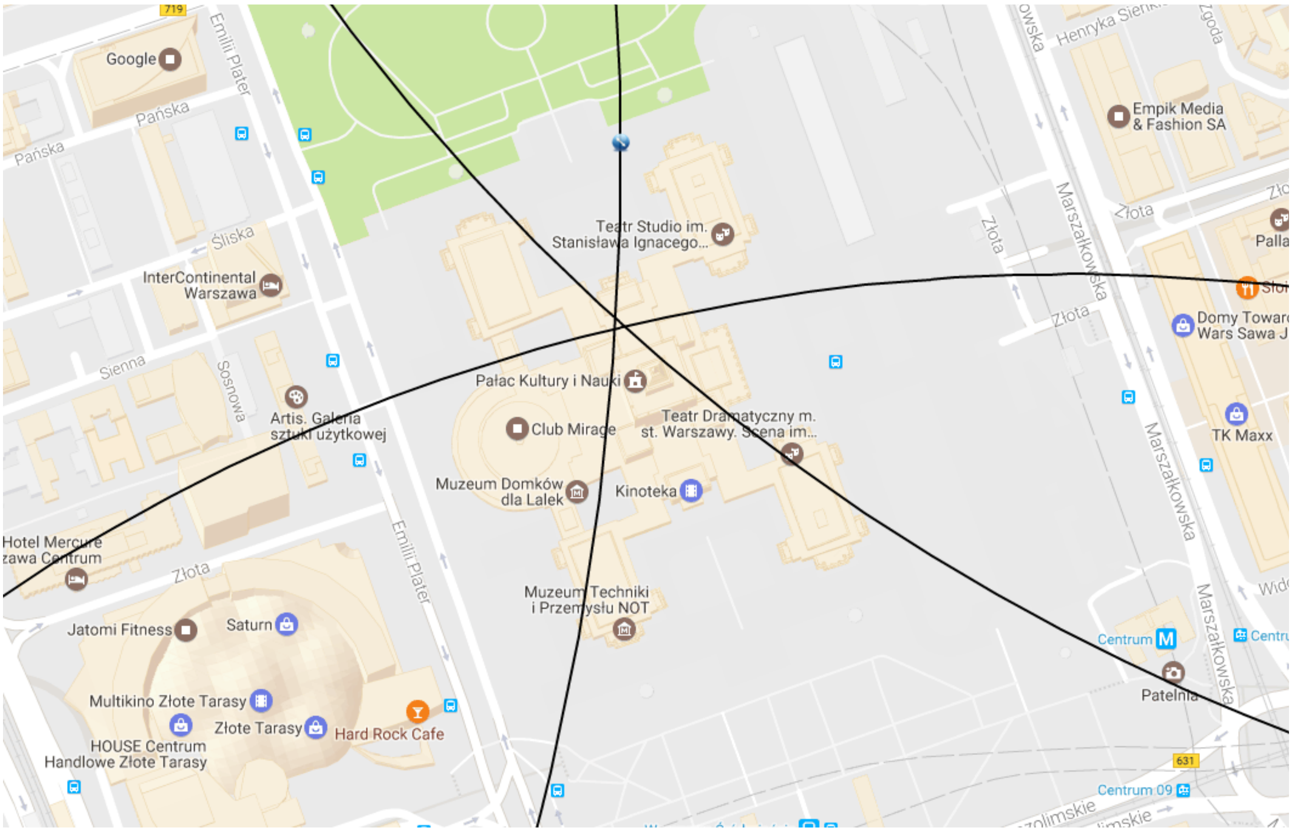


Illustration 4: Zoomed image of intersection point

Fixing vulnerability

Fixing vulnerabilities that result in the possibility of trilateration is not a trivial task. Many of popular mobile applications had problems with this vulnerability, even if fuzzing techniques have been implemented to reduce the accuracy of distance displayed. Many of these fuzzing techniques have been found vulnerable to complicated attacks leveraging use of statistics to determine the distortion cause by fuzzing.

Any solutions obstructing the access to API that returns user locations can be easily bypassed by Reverse Engineering techniques. The best solution would be to stop using geolocation features, but that is not always possible. The accuracy of trilateration can be reduced by providing the less accurate distance. It will still allow the attacker to find the location of a victim using more sophisticated attack.

More advanced solutions need to be implemented in order to make the trilateration less accurate. One of these methods is spatial cloaking discussed in *Where's Wally? Precise User Discovery Attacks in Location Proximity Services*[1] and *Spatial Cloaking for Anonymous Location-based Services in Mobile Peer-to-Peer Environments*[2].

[1] https://www.cs.uic.edu/~polakis/tr/proximity-tr.pdf

[2] http://www-users.cs.umn.edu/~mokbel/papers/geoinformatica10.pdf