Location Based Services – Bug or Feature

Term Paper

Chair for Communication Security
Ruhr-Universität Bochum

Michael Pridat

24.07.07

Content -1-

- Mobile phone as a bug
  - Basics
  - Mobile phone micro as eavesdropping tool
  - Requirements
    - Over the air programming
  - Realization via OTA mechanism

Content -2-

- Mobile phone localization for everyone
  - Basics
  - Locating technologies
    - Trilateration
    - Triangulation
    - TDOA and TOA
    - E-OTD, AOA and COO
  - Accuracy
  - LBS Provider
- Conclusion
- References
- Wikipedia

Mobile phone as a bug

Basics

- Overview of security vulnerabilities of a mobile phone.

(3) Vulnerability to monitoring of your conversations while using the phone.

(4) Vulnerability of your phone being turned into a microphone to monitor conversations in the vicinity of your phone while the phone is inactive.

- I will only describe the second vulnerability aspect.

Mobile phone as a bug

Mobile phone micro as eavesdropping tool

- According to various reports the FBI uses mobile phones as eavesdropping tool.
- For this, the software of the mobile telephones is reprogrammed. The free speech mechanism is activated without any users knowledge.
- The same modification of the mobile phones software uses the State Office of Criminal Investigation in Germany as Spiegel Online reports last week.

Mobile phone as a bug

Requirements

- Only one condition seems to be necessary for using a mobile phone as a bug. It had to be reprogrammable (over the air).

- A second requirement is not mandatory. A phone which is in stand by mode even though it is switched of is needed.

  (This can be easily identified, because these phones alarm clock function (e.g.) is still working even though the phone is switched off.)

Mobile phone as a bug

Requirements: OTA mechanism

- Definition of over the air programming

  OTA mechanism requires an existing software and hardware of the target device.

  OTA programming is a method of distributing new software updates.

  It is often necessary to turn the phone off and back on for the new programming to take effect, therefore many phones will automatically perform this action.

Mobile phone as a bug

Realization via OTA mechanism

- OTA update function is used to transfer “special" software which can offer one of the following features
  - Outgoing connections which are established by the “special” software are not shown on the mobile phones user interface.
  - The “special” software is able to accept an incoming connection w/o showing this on the mobile phones user interface.
  - If the phone gets switched off, the ”special” software only pretends this.
  - Even though the mobile phone gets switched off, it is in a standby comparable status and the “special” software is still working.
  - It is also possible to deposit an audio recording in the mobile phones internal buffer and send these recordings in batches.

Mobile phone localization for everyone

LBS: Basics

- Wherever mobile phone users stay, they are permanent accessable.

- As a result of this, many new options arise:
  - Users subscribe search functions for friends or their children.
  - Users can be sent information on the cell phone about shopping facilities or restaurants referring to their surrounding area.
  - Companies can monitor their car pool and field manager at the PC.

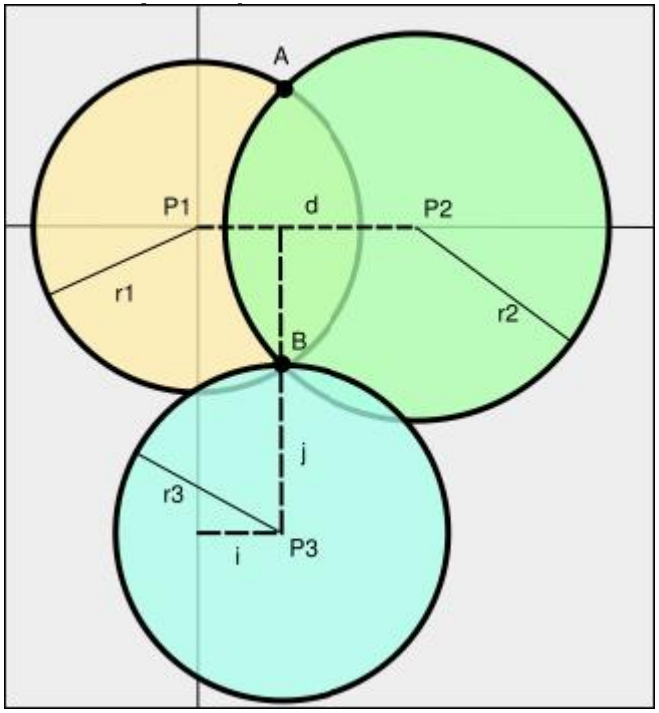
- All these LBS functions are based on the subscribers current location or personal data.

Mobile phone localization for everyone

Locating technology: Trilateration

- Two basic methods are used for localization.

- Trilateration (measuring the distance to known reference



Standing at (B)

Reference points are (P1), (P2), and (P3)

Measuring r1 narrows the position down to a circle

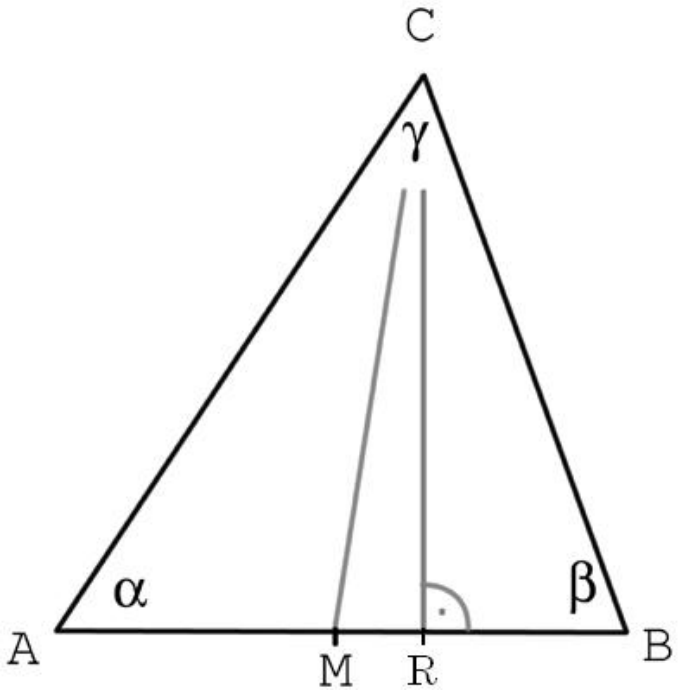
Measuring r2 narrows the position down to two points, (A) and (B)

Measuring r3 gives the coordinates at (B)

Mobile phone localization for everyone

Locating technology: Triangulation

- Triangulation (measuring the angle to known reference points)



α, β and distance AB are already known

C can be calculated in different ways:

- Position of RC can be calculated using law of sines and law of cosines
- MC can be calculated using Pythagorean theorem

Mobile phone localization for everyone

Locating technology: TDOA and TOA

- The most popular methods of position location capabilities are:

  Time Difference of Arrival (TDOA)

  - The network determines the time difference and therefore the distance from each tower to the mobile phone.

  Time of Arrival (TOA)

  - Same as TDOA but this technology uses the absolute time of arrival at a certain base station rather than the difference between two stations.

Mobile phone localization for everyone

Locating technology: E-OTD, AOA and COO

Enhanced Observed Time Difference -Technology (E-OTD)

- Similar to TDOA, but the position is estimated by the mobile phone, not by the base station.

Angle of Arrival (AOA)

- AOA mechanism locates the phone at the point where the lines along the angles from each tower intersect.

Cell of Origin (COO) (standard at German networks)

- The current cell location where the mobile phone is logged in is indicated.

Mobile phone localization for everyone

Accuracy

- Accuracy depends on the actual position and used localization technique.
- URBAN AREAS: Built up areas and cities such as Hamburg, Berlin, Ruhrgebiet can expect accuracy between 50m to 400m.
- SUBURBAN AREAS: Suburban areas vary between 450m and 2km.
- RURAL AREAS: Due to the sparse nature of the operator base stations in rural areas the accuracy can vary from 1.5km to 9km

Mobile phone localization for everyone

LBS provider

- Overview of tested LBS provider

Provider	Price (GSM)	Registration	Safety	Free localizations	Extras
www.corscience.de	49ct	Yes	SMS for activation	4	Google Earth Link / Interval localization
www.picosweb.de	49ct	Yes	SMS for activation / SMS Reply for confirmation	1	–
www.via-ferrata.de (based on picos)	99ct	Yes	SMS for activation / SMS Reply for confirmation	1	–
www.handy-ortung.5zu7.de (based on picos)	49ct	Yes	SMS for activation / SMS Reply for confirmation	1	–

- The localization results are comparable because all LBS provider in Germany are using the COO mechanism.

Conclusion

Phone as eavesdropping tool

- The only advice which is useful as counteraction, is to take out the rechargeable battery of the phone when sensitive information needs to be talked about.

Mobile phone localization

- Everyone can locate a foreign mobile phone using LBS provider.
- To prevent this you have to change frequently your mobile phone or SIM-Card with friends, colleagues or intimate or apply the first advice...

References

- http://news.com.com/FBI+taps+cell+phone+mic+as+eavesdropping+tool/2100-1029 3-6140191.html
- http://www.spiegel.de/netzwelt/tech/0,1518,494461,00.html
- http://en.wikipedia.org/wiki/Over-the-air programming
- http://www.mobilelocate.co.uk/accuracy.htm

Wikipedia

- http://en.wikipedia.org/wiki/GSM_localization
- http://en.wikipedia.org/wiki/Covert_listening_device