Yet another way to cause DoS for GSM devices

Domonkos P. Tomcsanyi

Agenda

- History of GSM DoS attacks
- Location Updates (LU)
- The attack

History of GSM DoS

- (jamming)
- RACHell (Dieter Spaar - 2009)
- IMSI detach (Sylvain Munaut - 2010)
- Paging race condition (Nico Golde - 2012)

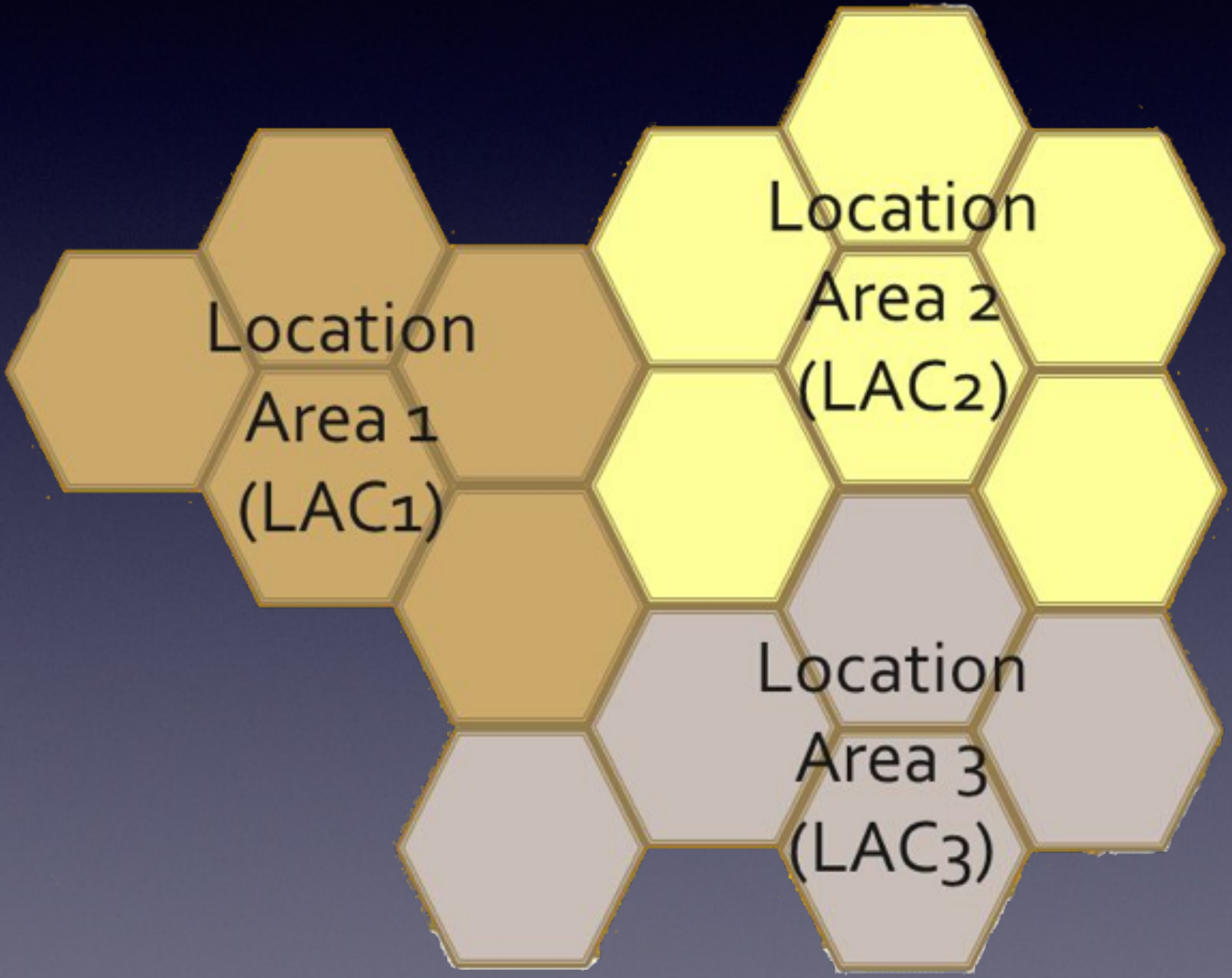
What’s the difference?

- This attack is:

  - targeted
  (from a single phone number to all phones in the range)

  - not necessary instantaneous (you can run away :)

Location Areas



Location Update (LU)

- When?
  - Phone switched on
  - Phone goes to a different Location Area
  - Phone is commanded to do a regular LU

LU Reject

- BTS could reject a Location Update Request for various reasons, for example:
  - Cause #13 - “roaming not allowed in LA”
  - Cause #2 - “IMSI unknown in HLR”
  - Cause #3 - “illegal MS” (SIM card problem)
  - Cause #6 - “illegal ME” (stolen phone)

How does a phone react?

- If the reject value is #11, #12, #13, or #15, the MS (…) sets the update state to Roaming Not Allowed.

- If the reject value is #2, #3, or #6, the MS sets the update state to Roaming Not Allowed (…) and considers the **SIM as invalid until it is switched off** or the **SIM is removed**.

- Other reject values are considered as abnormal cases (no reaction?).

What’s needed for the attack?

- We need to set up a fake base station
- We need to get phones to connect to it
- We need to make the connected phones to do a Location Update

Get a fake BTS

- OpenBSC, OsmoBTS and osmo-trx create a full implementation of a mobile network
- They support SDR (Software Defined Radio) hardware
- There is also support for using an OsmocomBB phone as base station
  -> it is limited, but it works well

How to get phones to hand-over?

Luring phones

- Hand-over is based on signal strength and signal quality (RSSI) - we need to be on the right frequency

- But there is one more thing: C1 and C2 algorithms: the cell-selection and re-selection process based on their output

- Both uses a value, CRO (cell reselection offset) which is broadcasted by the BTS

- Set CRO to a high value
  -> you are the **best tower**, (almost) **no matter how bad your signal is**

How high?

- First we set it to the maximum (126)
- iPhones did handover immediately, but other phones didn't
- \o to *short int* overflow
- OK, so around 40-50 it is great
- Actually we just built an IMSI-catcher :)

Luring phones

- We need the phone to initiate a LU (so we can reject it)
- We can set the Location Area Code of our BTS, so any phone that connects will do a LU automatically

The attack

- OsmocomBB phone as base-station
(any other supported SDR could be used)

- We can do many things:

  - make phones disable themselves in specific areas (cause #11, #12, #13, #15)

  - disable the phones around us until they are rebooted (cause #2, #3) or disable them permanently (?, cause #6)

DEMO

Warning! Your phones will be affected if you are on 2G/GSM.

Countermeasures?

- The concept is wrong in GSM (“the tower is trusted no matter what”)
- Use 3G/4G whatever

Ideas

- OK, phones could use 3G easily today
- How about other GSM-based systems?
  - House alarm systems, smart meters, traffic lights etc.
- How often are those rebooted/moved?

Conclusion

- GSM will probably survive 3G, maybe even 4G, because it is used by so many embedded systems
- It will always be the fallback/backup for phones

  -> still a good area to do research on, especially with the great tools we have

A huge applause for…

- Osmocom project as a whole, but especially:
  - BB
  - OpenBSC
  - OsmoBTS
  - OsmoTRX
- Sylvain Munaut, Andreas Eversberg, Dieter Spaar, Harald Welte, Nico Golde and so many others

Questions?

I’ll be in the speaker’s corner (Leisure Zone)

Thank you!

Used code will be available on github (@domi007)