Catching IMSI catchers

Or how we failed to find any.
IMSI’s?

- International Mobile Subscriber Identity
- Unique identity on mobile phone networks
- Rarely send over the network
IMSI catcher?

- Also known as Stingray in the U.S
- Device to eavesdrop on conversation
- Possibility for tracking movement
HOW ‘STINGRAY’ WORKS

The box-shaped portable device can track hundreds of phones at a time. It is made by Harris Corp., which sells it to law enforcement agencies but does not disclose information about it to the public.

Normal cellphone use

*Powered-on cellphones constantly look for the nearest cell tower, even if no call is being made.*

With the device

*Stingray sends out a signal that tricks cell phones into thinking it is a tower. Phones in the area connect to it without the user’s knowledge. Stingray collects data from the phones, and then passes the data on to the real tower.*

What it collects:

- Unique identifying numbers for all cellphones that connect to it. These numbers can be used to get historical data about phone calls, texts, and location.
- Numbers dialed by that cellphone, including those for outgoing texts.
- Location of the connected phones.
- Some models can capture voice communication, data, and text messages. The Sacramento County Sheriff’s Department stated that its device is not capable of this.

In the van:

*A laptop connected to the Stingray device translates and displays the captured information, allowing law enforcement to target specific phones.*
IMSI catcher catcher?

- Ways to detect silent text messages
- Ways to detect SS7 network attacks
- Ways to detect IMSI catchers
- Or: battery drain
Cryptophone
100 euro and a few hours

- Moto E (XT1021)
- Unlock + Root
- Install SnoopSnitch
- Not easy for average user
Driving around

- Amsterdam →
- Schiphol →
- Wageningen →
- The Hague
Nothing!

- Nothing interesting.
Schiphol?

- Nothing
SnoopSnitch results

- Not a single event.
  - No SS7 event
  - No IMSI-catcher
  - No silent text messages
  - No nuffin’
Cryptophone

- Lots of event.
- Lots of the same events.
- No useful data.
- Only detects baseband issues.
  - Not such a good measure.
  - Didn’t catch any NSA TAO 0day
Vodafone

- Doesn't seem to like silent sms
- SnoopSnitch not working fine enough?
- Need more cross-network data!
Future research

- Gather data from more providers.
- Use OsmocomBB C115.
- Correlate data sources.
  - Hard to pull off
Conclusions

- Were not on a shit list yet.
- Vodafone has a pretty fine network.
- KPN as well.
- Maybe too early?
What’s next?

● More research!
● Standard integration for Iphone/Android!
● Open source basebands……..
The end

- Thx: Douwe
- Contact: me@jurrevanbergen.nl