Project voorstel
Ilias, Jef, Zakaria, Lorik, Adrie

Onderzoeksvraag:

In hoeverre bestaan er kwetsbaarheden in GSM-communicatie die misbruikers in staat stellen om ongeautoriseerd af te luisteren of caller-ID te spoofen?

Gsm-communicatie afluisteren:

We gaan ons eigen telefoonbasisstation bouwen, waarmee alle GSMs in de buurt verbinding kunnen maken. Hiermee zullen we experimenten uitvoeren en proberen telefoongesprekken af te luisteren.

Benodigdheden:

- Full duplex SDR die die tot minstens 1900 Mhz aan kan. (**Adalm pluto** of **HackRf One x 2**)
- SDR software (GNU Radio)
- GSM x 2

(optioneel) SMS sturen met SDR:

Als ons eerste onderzoek met succes wordt uitgevoerd en we nog tijd over hebben, kunnen we beginnen aan ons tweede onderzoek. We kunnen proberen een SMS te verzenden met behulp van HackRF en Pluto zonder gebruik van een SIM-kaart. Als dit lukt, kunnen we ook proberen SMS-spoofing uit te voeren.

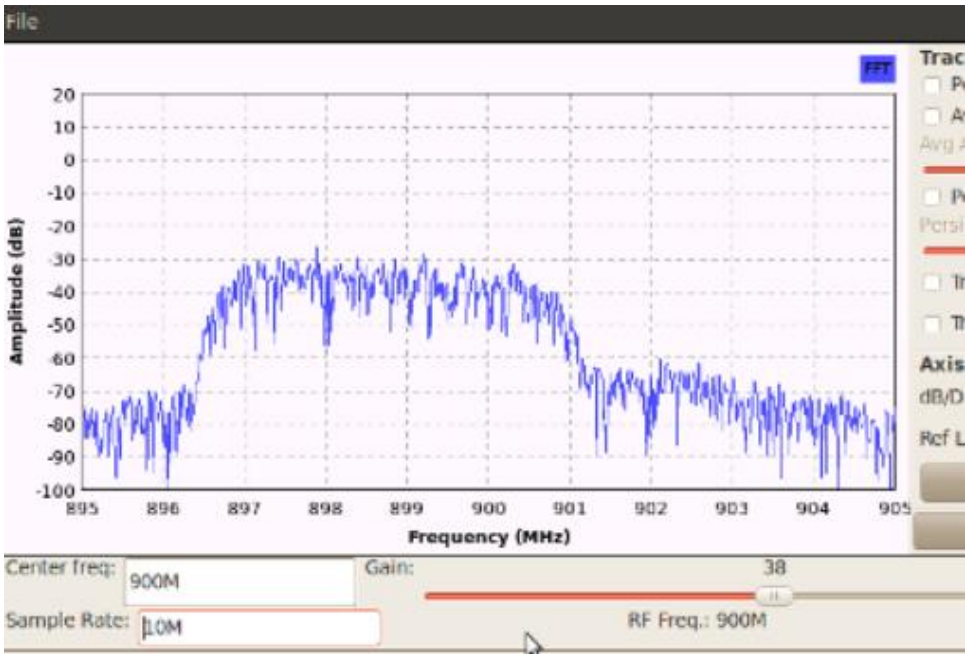
Benodigheden:

- SDR
- HackRF of ADALM-PLUTO
- SIM-kaart (liefst zonder SIM-kaart proberen maar dat is een uitdaging)
- SIM-kaart reader (indien SIM-kaart nodig)

Vooruitgang 1:

In de aanvangsfase van ons project hebben we onderzocht of het mogelijk was om 2G-communicatie te onderscheppen met behulp van onze RTL-SDR. We hebben twee GSM's op 2G ingesteld en GNU Radio gebruikt als SDR-software op Linux. Na diverse pogingen zijn we erin geslaagd de frequentie te

identificeren waarop onze twee GSM's met elkaar communiceren. Tijdens het opnemen en verbreken van de GSM-verbindingen observeerden we een verschil in het grafische overzicht.



Een potentieel probleem dat zich voordoet, is dat RTL-SDR een maximaal bereik heeft van 1.75 GHz terwijl 2G eigenlijk op ook op 1800 MHz kan communiceren. Dit vormt een uitdaging voor ons project.

Momenteel zijn we nog steeds op zoek naar geschikte SDR-software voor HackRF die zo veel mogelijk GSM-ondersteuning biedt. Hoewel we OpenBTS hebben overwogen, ondervonden we helaas veel compatibiliteitsproblemen met HackRF. We zoeken nu naar alternatieve oplossingen.