Project voorstel

Contributors: Ilias, Jef, Zakaria, Lorik, Adrian

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 1800 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 SMSspoofing 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)

Wireless technologies SDR project

Geschiedenis:

2G/GSM (1991):

- **Introductie van Digitale Communicatie**: 2G, ook bekend als GSM (Global System for Mobile Communications), markeerde een overgang van analoge naar digitale communicatie. Het maakte niet alleen draadloze gesprekken mogelijk, maar ook tekstberichten (SMS), waardoor de mobiele communicatie aanzienlijk werd verbeterd.
- **Internationale Roaming**: Een belangrijk kenmerk van GSM was de mogelijkheid tot internationale roaming, waardoor gebruikers hun mobiele telefoon in verschillende landen konden gebruiken zonder van nummer te veranderen.

3G/UMTS (2001):

- **Snellere Gegevensoverdracht en Internettoegang**: De introductie van 3G (Universal Mobile Telecommunications System - UMTS) betekende een aanzienlijke verbetering van gegevensoverdrachtssnelheden. Gebruikers konden nu niet alleen spraakoproepen doen en sms'en, maar ook internetdiensten gebruiken, zoals mobiel browsen en e-mailen.

4G/LTE (2009):

- **Hogere Snelheden en Efficiëntie**: 4G, met name LTE (Long-Term Evolution), bracht aanzienlijk hogere datasnelheden en efficiëntie in vergelijking met 3G. Dit maakte de soepele werking van veeleisende toepassingen zoals streaming video en online gaming mogelijk.

Informatie:

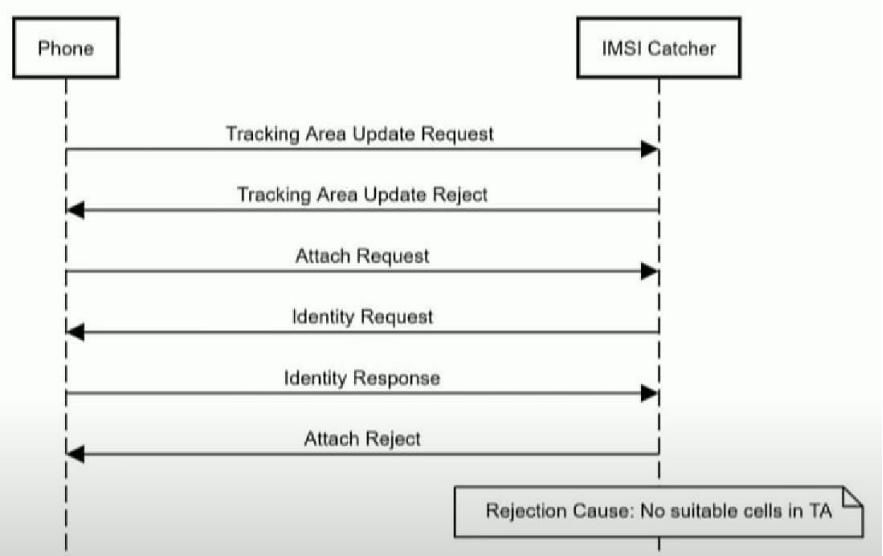
Hoe wordt bepaald met welke base station de mobiel verbindt?

1. **Cell reselection**: Mobiele apparaat meten voortdurend de signalen van base stations in de buurt. Als de metingen aangeven dat een andere base station mogelijk een betere verbinding biedt, wordt een handover overwogen.
2. **Measurment report**: Het mobiele apparaat stuurt periodiek meetrapporten naar de huidige base station (waarmee het is verbonden). Deze rapporten bevatten informatie over de sterkte en kwaliteit van signalen van base stations in de buurt
3. **Event triggering:** op basis van de meetrapporten, kan een handover worden geactiveerd. De handover kan bijvoorbeeld plaatsvinden als de priority frequency hoger is of als de signaalsterkte van een base station beter is.
4. **Handover Decision**: De base station in het netwerk neemt de uiteindelijke beslissing over de handover. Het kan de handover goedkeuren of afwijzen op basis van zijn eigen evaluatie van de netwerkcondities en belasting.

Wat is een IMSI catcher?

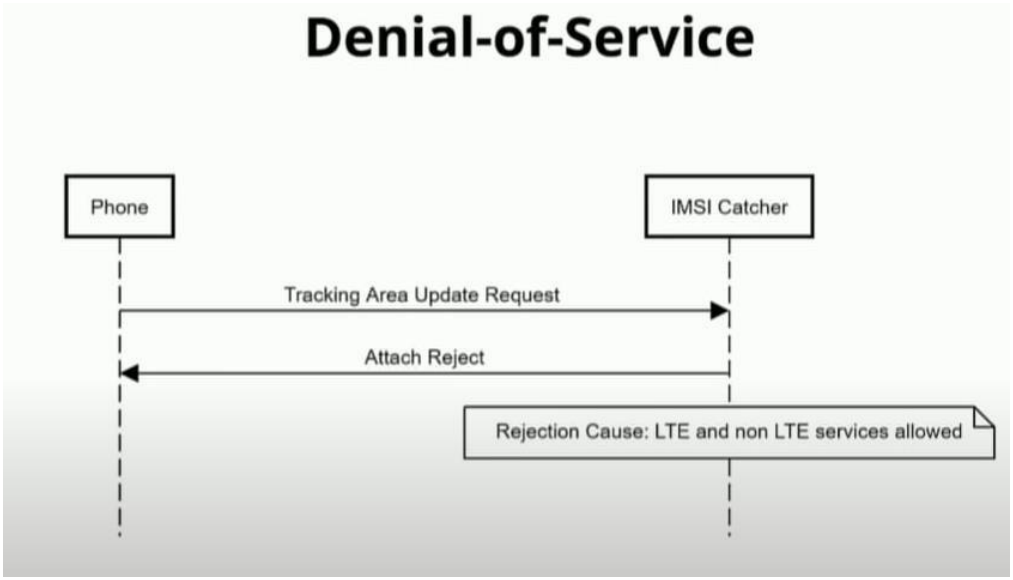
- Een IMSI-catcher, wat staat voor "International Mobile Subscriber Identity catcher," is een apparaat dat wordt gebruikt om mobiele telefoons te volgen en te identificeren. Het apparaat werkt door zich voor te doen als een legitieme mobiele zendmast, waardoor mobiele telefoons in de buurt ermee verbinding proberen te maken. Zodra een mobiel apparaat zich verbindt met de IMSI-catcher, kan de IMSI-catcher de unieke identificatiegegevens van het apparaat verzamelen.

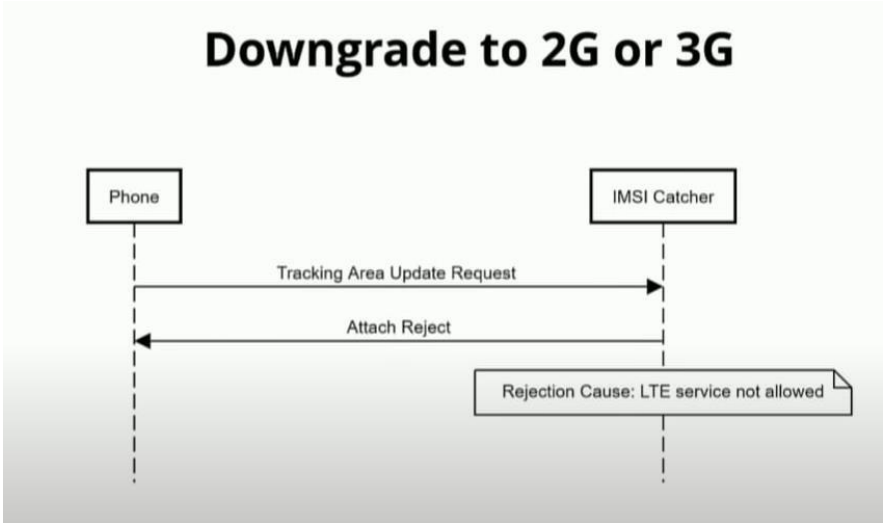
Welke berichten worden er overgedragen bij het opzetten van een IMSI catcher?



Wat zijn de gevaren van een IMSI catcher?

- **Afluisteren van communicatie:**
  - IMSI catchers kunnen proberen de communicatie tussen mobiele apparaten en het netwerk te onderscheppen. Dit kan het afluisteren van telefoongesprekken, sms-berichten en andere gevoelige informatie mogelijk maken.
- **Verstoring van dienstverlening:**
  - IMSI catcher kan een denial-of-service uitvoeren. Wanneer je in de attach reject message volgende prompt toevoegd: **“Rejection Cause: LTE and non LTE services allowed”,** zal het toestel niet meer naar andere base stations zoeken en gaat het in *ghost mode*. Todat het toestel reboot, zal deze in deze mode blijven.

- 

- **Downgraden van radiotechnologie:**
  - Een IMSI catcher kan een toestel dat verbonden is met 4G/LTE, downgraden naar 2G of 3G. Dit kan doormiddel van volgende prompt in attach reject message toe te voegen: **“Rejection Cause: LTE service not allowed”**.
  - 

- **Locatietracking:**
  - Door de sterkte van het mobiele signaal te meten, kunnen IMSI-catchers de locatie van mobiele apparaten bij benadering bepalen. Dit kan worden misbruikt voor ongewenst locatietracking. Zo kunnen bijvoorbeeld inbrekers zien of iemand thuis is of niet.
- **Mobiel nummer spoofen:**
  - De IMSI catcher ontvangt allerlei informatie waaronder de IMSI nummer, SMSC (Short message service center) nummer en sender ID. Door deze te ontvangen kun je via iemands anders nummer bellen en sms sturen.

Ons voorbereiden

Vooraleer we een eigen IMSI catcher willen opzetten, zullen we eerst heel wat moeten voorbereiden.

Besturingssysteem

- Bij het kiezen van een besturingssysteem, moet je goed kijken wat je precies wilt doen. We hebben gekozen voor Kali linux omdat dit veel makkelijker is dan windows.

Software

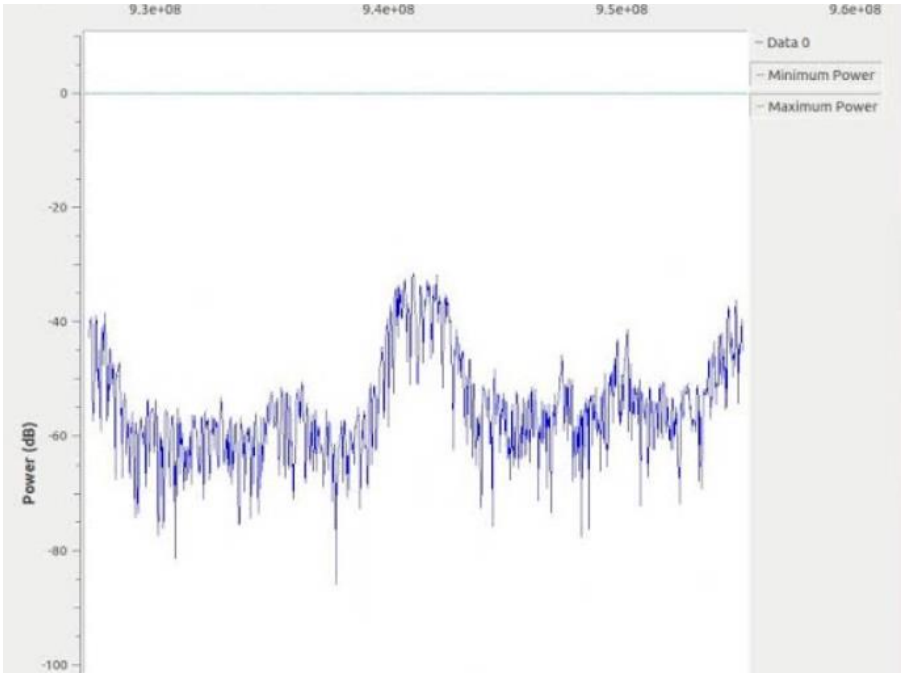
- Gr-gsm
- IMSI-catcher
- Dependencies:
  ○ cmake ○ autoconf ○ libtool ○ pkg-config ○ build-essential ○ python-docutils ○ libcppunit-dev ○ swig ○ doxygen ○ liblog4cpp5-dev ○ gnuradio-dev ○ gr-osmosdr ○ libosmocore-dev ○ liborc-0.4-dev

Hardware

- Computer
- SDR
- Antennes
- Mobiele apparaten
- SIM-kaart

Hands-on

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 gr-gsm gebruikt 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.



We hebben ook geprobeerd om de IMSI-nummer te catchen met behulp van een python script, maar helaas wilde onze IMSI-catcher niet werken. We zullen tegen volgende week samen onderzoeken hoe we dit kunnen oplossen en zo (onze eigen) IMSI's onderscheppen zodat we verder kunnen met de volgende fases.

Uitdagingen:

Een potentieel probleem dat zich kan voordoen bij ons project, is dat RTL-SDR een maximaal bereik heeft van 1.75 GHz terwijl 2G eigenlijk ook op 1800 MHz kan communiceren. Dit vormt een uitdaging voor ons project. Gelukkig communiceert onze GSM's voorlopig op 900MHz, maar dit is natuurlijk afhankelijk van de GSM en de provider.

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.

Hulpbronnen:

Handover protocol in LTE https://www.linkedin.com/pulse/handover-lte-techlte-world/

Hacking 4G and how to get arrested in 10 minutes - Christian Sørseth https://youtu.be/DEeOFE_DreU?si=3ARq0OqYU-7wPpSf Gr-gsm https://github.com/bkerler/gr-gsm

Stingray/IMSI Catchers: The Frightening Reality of Mobile Phone Surveillance

https://youtu.be/LSQIs4PujCQ?si=68grFR_94ZmM4kxv A VIDEO

DEMONSTRATION ON CRACKING A GSM CAPTURE FILE

https://www.rtl-sdr.com/tag/cellular/ Cellmapper https://www.cellmapper.net/arfcn Hackers-arise

https://www.hackers-arise.com/post/software-defined-radio-part-6-building-a-imsi-catcher-stingray

IMSI-catcher https://github.com/Oros42/IMSI-catcher