BEST Laboratorium Ćwiczenie 5: Nasłuchiwanie sieci GSM

Autorzy: Piotr Szewczyk, Paweł Murdzek

Cel ćwiczenia Celem ćwiczenia jest nasłuchiwanie sieci GSM (nie UMTS, LTE!) za pomocą taniego interfejsu RTL-SDR. W wyniku takiego nasłuchu możliwe jest odczytanie 1. Parametrów konfiguracyjnych stacji bazowych znajdujących się w okolicy terminal zrealizowanego za pomocą interfejsu RT-SDR 2. Odczyt wiadomości sygnalizacyjnych 3. Ewentualne wychwycenie numeru IMSI terminali (zamiast TMSI).

W trakcie realizacji laboratorium używaliśmy systemu DragonOS, który jest rozszerzeniem systemu Ubuntu z preinstalowanymi narzędziami do zajmowania się RF. Wcześniej próbowaliśmy zainstalować pakiet grgsm na zwykłym Ubuntu, ale najprawdopodobniej biblioteki są już przestarzałe i niekompatybilne. Zaczęliśmy więc od przeskanowania pasma GSM komendą grgsm_scanner -v. Oto część output'u i część tabeli ze znalezionymi stacjami:

```
piotrog@piotrog-VirtualBox:~$ grgsm_scanner -v

Try scan CCCH on 975-1023 arfcn`s:
Scanning: 0.00% done..

Found CCCH arfcn: 975
Dont capture immediate assignments, skip extract SDCCH/8 info and scan...
ARFCN:  975, Freq:  925.2M, CID:     0, LAC:  1480, MCC: 260, MNC:   6, Pwr: -45
  |---- Configuration: Unknown
  |---- Cell ARFCNs:
  |---- Neighbour Cells:


Found CCCH arfcn: 977
Dont capture immediate assignments, skip extract SDCCH/8 info and scan...
ARFCN:  977, Freq:  925.6M, CID: 16689, LAC:  1480, MCC: 260, MNC:   6, Pwr: -27
  |---- Configuration: 1 CCCH, combined
  |---- Cell ARFCNs: 975, 977
  |---- Neighbour Cells: 611, 613

Scanning: 20.00% done..
```

Rysunek 1 grgsm_scanner -v

Tabela 1 Znalezione stacje bazowe

ARFCN	Frequency (MHz)	CID	LAC	MCC	MNC	Power (dBm)
975	925.2	0	1480	260	6	-45
977	925.6	16689	1480	260	6	-27
13	937.6	22201	11001	260	1	-29
10	937.0	23591	11001	260	1	-30
94	953.8	0	58120	260	3	-28
124	959.8	29027	58120	260	3	-25
3	935.6	15051	11022	260	1	-32
998	929.8	16523	1480	260	6	-38
47	944.4	41972	58120	260	2	-39

43	943.6	822	11022	260	1	-26
48	944.6	14027	58120	260	2	-44
89	952.8	29023	58120	260	2	-25
92	953.4	2116	58120	260	3	-31
121	959.2	14030	58120	260	3	-44
123	959.6	2661	58120	260	3	-37

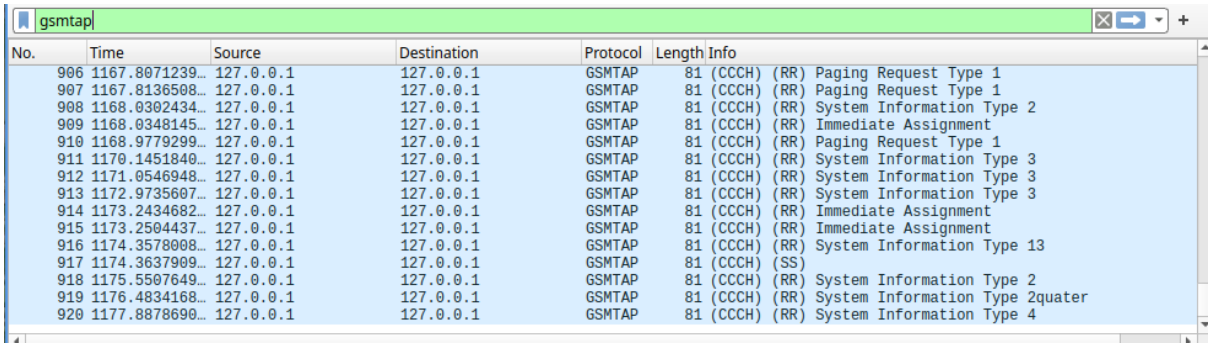
W analizowanym ruchu sygnalizacyjnym oraz w raportach skanowania pojawiają się kluczowe parametry i skróty, które charakteryzują sieć GSM oraz identyfikują stacje bazowe i terminale.

- **ARFCN (Absolute Radio-Frequency Channel Number):** Absolutny Numer Kanału Radiowego. Jest to unikalny numer przypisany do pary częstotliwości radiowych (jednej dla nadawania od stacji bazowej do terminala – *downlink* – i jednej dla nadawania od terminala do stacji bazowej – *uplink*). Każda stacja bazowa nadaje sygnał na jednym lub kilku ARFCN-ach w swojej komórce.
- **CID (Cell ID):** Identyfikator Komórki (Cell Identity). Jest to unikalny numer identyfikujący konkretną komórkę (sektor stacji bazowej) w ramach danego obszaru lokalizacji (LAC). Służy do rozróżniania komórek w tym samym LAC.
- **LAC (Location Area Code):** Kod Obszaru Lokalizacji. Sieć komórkowa jest logicznie podzielona na obszary lokalizacji, z których każdy ma swój unikalny kod LAC. Terminal informuje sieć o swojej lokalizacji, gdy zmienia LAC, co pozwala sieci efektywnie zlokalizować go w celu dostarczenia połączeń czy wiadomości.
- **MCC (Mobile Country Code):** Kod Kraju Sieci Komórkowej. To trzycyfrowy kod, który jednoznacznie identyfikuje kraj, w którym działa operator sieci komórkowej. Dla Polski, MCC to 260.
- **MNC (Mobile Network Code):** Kod Sieci Komórkowej. Jest to dwu- lub trzycyfrowy kod, który w połączeniu z MCC jednoznacznie identyfikuje konkretnego operatora sieci komórkowej w danym kraju. Przykłady dla Polski to: 1 (lub 01 dla sieci Plus), 2 (lub 02 dla T-Mobile), 3 (lub 03 dla Orange), 6 (lub 06 dla Play).
- **TMSI (Temporary Mobile Subscriber Identity):** Tymczasowy Identyfikator Abonenta Mobilnego. Jest to dynamicznie przydzielany, losowy numer używany przez sieć do identyfikacji terminala. Służy on głównie do ochrony prywatności

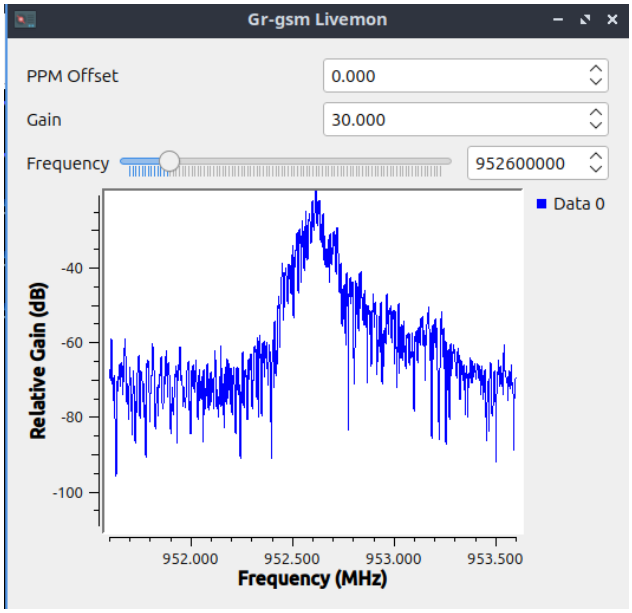
abonenta, ponieważ jest regularnie zmieniany i uniemożliwia łatwe śledzenie telefonu w eterze.

- **IMSI (International Mobile Subscriber Identity):** Międzynarodowy Identyfikator Abonenta Mobilnego. Jest to unikalny, stały numer przypisany do karty SIM użytkownika. Składa się z MCC, MNC oraz numeru identyfikacyjnego abonenta (MSIN). W przeciwieństwie do TMSI, IMSI jest rzadko przesyłane w eterze – głównie podczas pierwszej rejestracji telefonu w sieci, po długim czasie bezczynności lub w przypadku problemów z identyfikacją za pomocą TMSI.

Kolejnym krokiem była analiza wybranej stacji bazowej. Za pomocą komendy *grgsm_livemon*, byliśmy w stanie wybrać częstotliwość, na której będziemy odbierać pakiety GSMTAP za pomocą Wireshark'a. Udało nam się jedynie na częstotliwości około 952MHz znaleźć pakiety z kanału 977.



Rysunek 2 pakiety GSMTAP



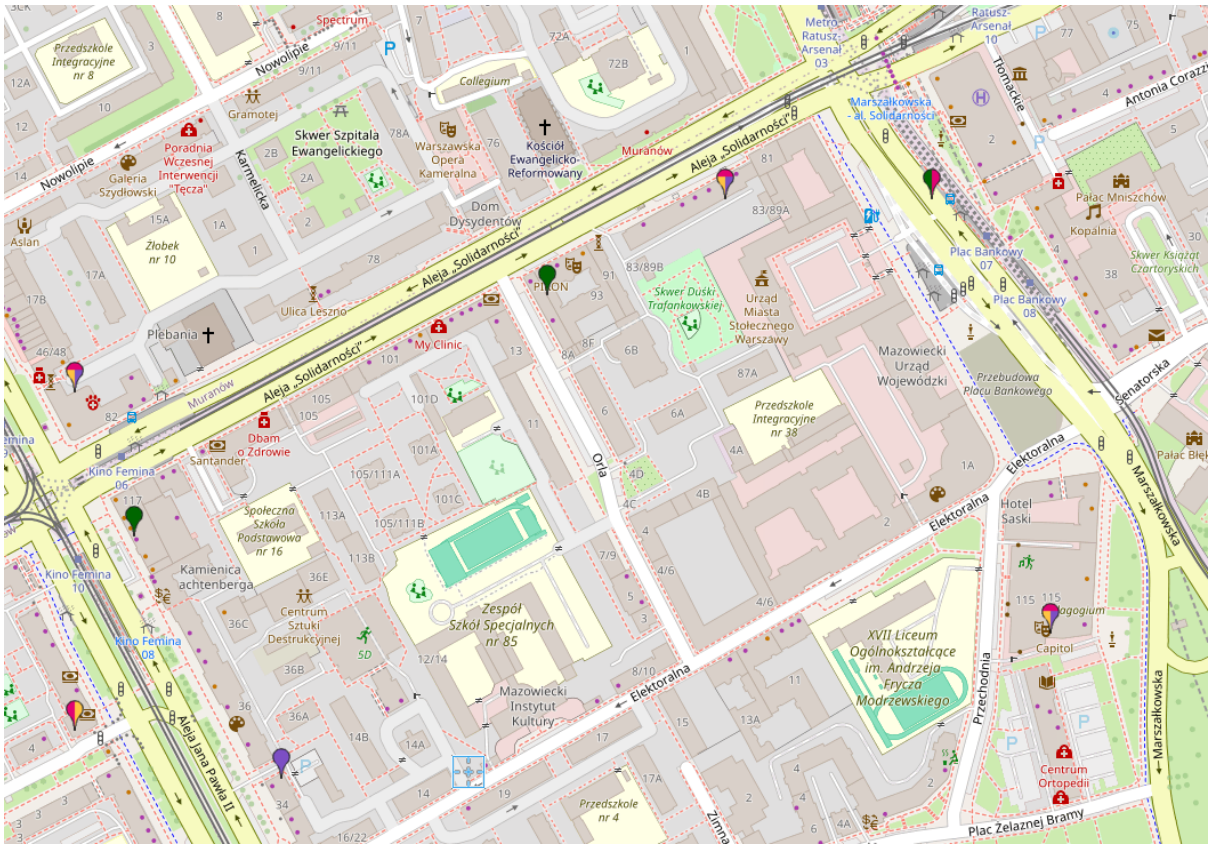
Rysunek 3 Wybrana częstotliwość

W trakcie monitorowania sygnalizacji sieci GSM podjęto liczne próby zidentyfikowania sytuacji, w której terminal mógłby transmitować swój stały identyfikator IMSI, zamiast tymczasowego TMSI. Pomimo wielokrotnych wymuszeń ponownej rejestracji telefonu w sieci (poprzez włączanie/wyłączanie trybu samolotowego oraz restart urządzenia), nie udało się zaobserwować transmisji IMSI. Terminal konsekwentnie przesyłał swój tymczasowy identyfikator TMSI, co świadczy o skutecznym działaniu mechanizmów ochrony prywatności w sieci GSM, która priorytetyzuje użycie TMSI, aby utrudnić śledzenie abonentów.

```
GSM TAP Header, ARFCN: 977 (Downlink), TS: 0, Channel: CCCH (1)
    Version: 2
    Header Length: 16 bytes
    Payload Type: GSM Um (MS <-> BTS) (1)
    Time Slot: 0
    ARFCN: 977
    Uplink: 0
    Signal Level (dBm): -27
    Signal Noise Ratio (dB): 0
    GSM Frame Number: 1061326
    Sub-Slot: 2
GSM Common Control Channel (CCCH) Paging Request Type 1
    L2 Pseudo Length: 12
    Protocol discriminator: Radio Resources Management messages (0x6)
    Message Type: CM Service Request (0x21)
    Ciphering Key Sequence Number: 7
    Mobile Station Classmark 1: R99, VBS, VGCS, A5/1, ...
    Mobile Identity
        Element ID: 0x17
        Length: 5
        1111 .... = Unused: 0xf
        .000 = Mobile Identity Type: TMSI/P-TMSI/M-TMSI (4)
        TMSI/P-TMSI: 0x44c5a847
    Service Type: Mobile originating calls (1)
```

Rysunek 4 Fragment z dekodowanego pakietu Wireshark (znalezione TMSI)

Kolejnym krokiem było znalezienie w obszarze skanowania stacji bazowych, które wykrył skaner. Laboratorium wykonywane było niedaleko ulicy Elektoralnej w Warszawie.



Rysunek 5 Mapa stacji bazowych (okolice Elektoralnej)

Przykład trzech odnalezionych stacji, które wcześniej wykrył skaner.

Play (26006) ID: WAR1019
Warszawa - Śródmieście, al. Solidarności 82 (dach - budynek mieszkalny)

GSM

Pasmo	LAC	CID	Uwagi
900	1480	16521	[E-GSM]
900	1480	16522	[E-GSM]
900	1480	16523	[E-GSM]

ARFCN	Frequency (MHz)	CID	LAC	MCC	MNC	Power (dBm)
998	929.8	16523	1480	260	6	-38

Rysunek 6 Stacja nr.1

Plus (26001) ID: BT14648

Warszawa - Śródmieście, al. Solidarności 117 (budynek Centrum Biurowego Bipromasz)

5G

Pasmo	Duplex	Uwagi
2600	TDD	--

GSM

Pasmo	LAC	CID	Uwagi
900	11022	15051	--
900	11022	15052	--
900	11022	15053	--

ARFCN	Frequency (MHz)	CID	LAC	MCC	MNC	Power (dBm)
3	935.6	15051	11022	260	1	-32

Rysunek 7 Stacja nr.2

T-Mobile (26002) ID: 20509 (N!)

Warszawa - Śródmieście, ul. Marszałkowska 115 (dach budynku - Teatr Capitol, Pedagogium WSNS)

5G

Pasmo	Duplex	Uwagi
3500	TDD	NetWorks

GSM

Pasmo	LAC	CID	Uwagi
900	58120	29022	NetWorks
900	58120	29023	NetWorks
900	58120	29024	NetWorks

ARFCN	Frequency (MHz)	CID	LAC	MCC	MNC	Power (dBm)
89	952.8	29023	58120	260	2	-25

Rysunek 8 Stacja nr.3