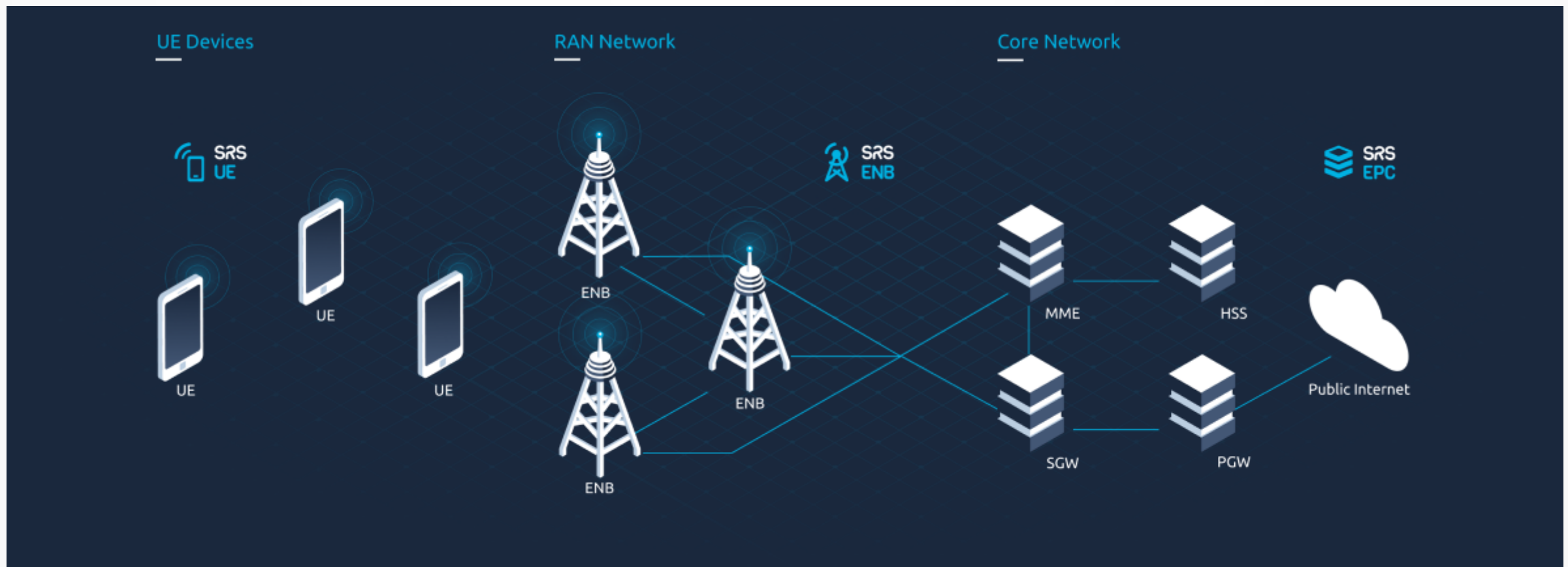




# LTE/4G/5G jak postavit a jak (od)poslouchat

**Postavení vlastní LTE “bejsky”, jak poslouchat  
traffic, o IMSI catcherech, downgrade a jiných  
útocích**

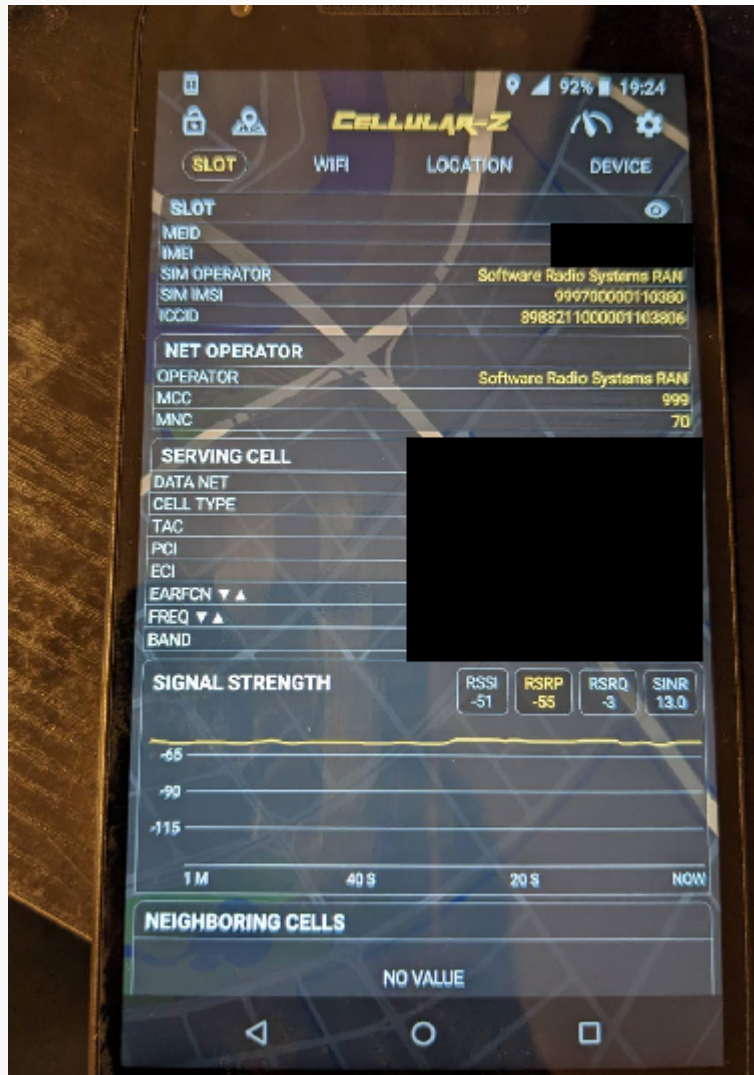
# 4G RAN – radio access network



# Jak postavit LTE “bejsku”?

- “Nejjednodušší” je SrsRAN projekt
  - BladeRF, B210 (i klony) funkční
  - proboha ne PlutoSDR, má chyb na čtvrtroku “tmy a smutna”
- Rádioová část SDR dělá **eNB**
  - pozor ale co kde vysíláte jak, zahrabat se hluboko s Faraday klecí – zákony, ČTÚ...
- Telefon je **UE** (user equipment), taky lze SrsRANem
- V pozadí je **EPC** (LTE core network)
  - napojeno na internet ven
  - všechny další věci jako mapping účastník-klíč-šifra, roaming
  - řešení sdílení v případě nouze (MOCN, MORAN...)

# LTE “bejska” i s EPC s COTS UE



COTS = “commercial off the shelf”  
Vlastní SIMky vyžadovány



# Bizáry 4G/LTE

- Bez VoLTE budou hovory přes 2G
- Vůbec se spoléhá na to, že všechno podle možnosti pojde přes data
- SMS jsou taky implementačně radost

# Sniffing LTE

- LTESniffer projekt
  - downlink z eNB bejsek control traffic nešifrovaný
  - na uplink to chce 2 SDR a ideálně GPSDO
- Soudruzi konečně použili AES na data
  - ne zabackdoorované šifry jako u 2G a 3G
  - teoreticky podporuje “žádné šifrování, =0”
  - ale **žádný telefon neakceptuje “žádná integrita, =0”**
  - AES použili špatně (CTR, bez MAC)
  - integrita v 4G i 5G je nevímproč 32-bit místo 128-bit když už AES-128

# Sniff (RNTI, TMSI, modulare 1)

| Num | RNTI  | Table  | Active | New TX | ReTX | Success   | HARQ | Normal | W_MIMO | W_pinfor | Othe |
|-----|-------|--------|--------|--------|------|-----------|------|--------|--------|----------|------|
| 1   | 18210 | 64QAM  | 11     | 11     | 0    | 6 (55%)   | 0    | 0      | 0      | 0        | 0    |
| 2   | 18342 | 64QAM  | 4      | 4      | 0    | 4 (100%)  | 0    | 0      | 0      | 0        | 0    |
| 3   | 18378 | 64QAM  | 10     | 10     | 0    | 10 (100%) | 0    | 0      | 0      | 0        | 0    |
| 4   | 18436 | 64QAM  | 7      | 7      | 0    | 5 (71%)   | 0    | 0      | 0      | 0        | 0    |
| 5   | 18490 | 64QAM  | 2      | 2      | 0    | 2 (100%)  | 0    | 0      | 0      | 0        | 0    |
| 6   | 18576 | 64QAM  | 16     | 16     | 0    | 12 (75%)  | 0    | 0      | 0      | 0        | 0    |
| 7   | 18647 | 64QAM  | 3      | 3      | 0    | 3 (100%)  | 0    | 0      | 0      | 0        | 0    |
| 8   | 18730 | 64QAM  | 9      | 9      | 0    | 9 (100%)  | 0    | 0      | 0      | 0        | 0    |
| 9   | 18895 | 64QAM  | 19     | 19     | 0    | 18 (95%)  | 0    | 0      | 0      | 0        | 0    |
| 10  | 18946 | 64QAM  | 7      | 7      | 0    | 5 (71%)   | 0    | 0      | 0      | 0        | 0    |
| 11  | 19037 | 64QAM  | 7      | 7      | 0    | 7 (100%)  | 0    | 0      | 0      | 0        | 0    |
| 12  | 19089 | 64QAM  | 16     | 16     | 0    | 4 (25%)   | 0    | 0      | 0      | 0        | 0    |
| 13  | 19256 | 64QAM  | 20     | 20     | 0    | 6 (30%)   | 0    | 0      | 0      | 0        | 0    |
| 14  | 19285 | 64QAM  | 13     | 13     | 0    | 10 (77%)  | 0    | 0      | 0      | 0        | 0    |
| 15  | 19381 | 64QAM  | 31     | 31     | 0    | 8 (26%)   | 0    | 0      | 0      | 0        | 0    |
| 16  | 19426 | 64QAM  | 16     | 16     | 0    | 8 (50%)   | 0    | 0      | 0      | 0        | 0    |
| 17  | 19428 | 64QAM  | 3      | 3      | 0    | 3 (100%)  | 0    | 0      | 0      | 0        | 0    |
| 18  | 19555 | 64QAM  | 4      | 4      | 0    | 4 (100%)  | 0    | 0      | 0      | 0        | 0    |
| 19  | 19588 | 64QAM  | 13     | 13     | 0    | 4 (31%)   | 0    | 0      | 0      | 0        | 0    |
| 20  | 19644 | 64QAM  | 13     | 13     | 0    | 12 (92%)  | 0    | 0      | 0      | 0        | 0    |
| 21  | 19675 | 64QAM  | 10     | 10     | 0    | 7 (70%)   | 0    | 0      | 0      | 0        | 0    |
| 22  | 19760 | 64QAM  | 13     | 13     | 0    | 6 (46%)   | 0    | 0      | 0      | 0        | 0    |
| 23  | 19819 | 64QAM  | 10     | 10     | 0    | 8 (80%)   | 0    | 0      | 0      | 0        | 0    |
| 24  | 19859 | 64QAM  | 10     | 10     | 0    | 3 (30%)   | 0    | 0      | 0      | 0        | 0    |
| 25  | 19933 | 64QAM  | 2      | 2      | 0    | 2 (100%)  | 0    | 0      | 0      | 0        | 0    |
| 26  | 19943 | 64QAM  | 4      | 4      | 0    | 3 (75%)   | 0    | 0      | 0      | 0        | 0    |
| 27  | 19967 | 64QAM  | 10     | 10     | 0    | 8 (80%)   | 0    | 0      | 0      | 0        | 0    |
| 28  | 20002 | 64QAM  | 2      | 2      | 0    | 2 (100%)  | 0    | 0      | 0      | 0        | 0    |
| 29  | 20102 | 64QAM  | 9      | 9      | 0    | 4 (44%)   | 0    | 0      | 0      | 0        | 0    |
| 30  | 20117 | 64QAM  | 35     | 35     | 0    | 23 (66%)  | 0    | 0      | 0      | 0        | 0    |
| 31  | 20169 | 64QAM  | 9      | 9      | 0    | 2 (22%)   | 0    | 0      | 0      | 0        | 0    |
| 32  | 18304 | 256QAM | 18     | 18     | 0    | 17 (94%)  | 0    | 0      | 0      | 0        | 0    |
| 33  | 18321 | 256QAM | 1427   | 1427   | 0    | 91 (6%)   | 0    | 0      | 0      | 0        | 0    |
| 34  | 18514 | 256QAM | 42     | 42     | 0    | 26 (62%)  | 0    | 0      | 0      | 0        | 0    |
| 35  | 18586 | 256QAM | 5      | 5      | 0    | 4 (80%)   | 0    | 0      | 0      | 0        | 0    |
| 36  | 18763 | 256QAM | 13     | 13     | 0    | 12 (92%)  | 0    | 0      | 0      | 0        | 0    |
| 37  | 18775 | 256QAM | 21     | 21     | 0    | 14 (67%)  | 0    | 0      | 0      | 0        | 0    |
| 38  | 18791 | 256QAM | 2      | 2      | 0    | 2 (67%)   | 0    | 0      | 0      | 0        | 0    |

# Sniff (RNTI, TMSI, modulare 2)

| SF     | Detected Identity     | Value     | RNTI  | From Message         |
|--------|-----------------------|-----------|-------|----------------------|
| 512 -9 | TMSI                  | f568c941  | 65534 | Paging               |
| 516 -9 | TMSI                  | f0733304  | 65534 | Paging               |
| 525 -9 | TMSI                  | d6c5f54f  | 65534 | Paging               |
| 527 -9 | TMSI                  | dabc0199  | 65534 | Paging               |
| 553 -9 | TMSI                  | c7871993  | 65534 | Paging               |
| 553 -9 | TMSI                  | ea4e7b13  | 65534 | Paging               |
| 555 -9 | TMSI                  | cbfc4723  | 65534 | Paging               |
| 569 -9 | TMSI                  | ebf509cf  | 65534 | Paging               |
| 598 -9 | TMSI                  | ec2cecebe | 65534 | Paging               |
| 606 -9 | TMSI                  | e7c8f314  | 65534 | Paging               |
| 613 -9 | TMSI                  | f43e8f8f  | 65534 | Paging               |
| 614 -9 | TMSI                  | e2f7f2cc  | 65534 | Paging               |
| 628 -9 | TMSI                  | e6d92704  | 65534 | Paging               |
| 629 -9 | TMSI                  | d2f9a066  | 65534 | Paging               |
| 642 -9 | TMSI                  | edaf3110  | 65534 | Paging               |
| 647 -9 | TMSI                  | dc207721  | 65534 | Paging               |
| 653 -9 | TMSI                  | f42365a8  | 65534 | Paging               |
| 655 -9 | TMSI                  | d4bf85f2  | 65534 | Paging               |
| 718 -9 | TMSI                  | f72a0aed  | 65534 | Paging               |
| 721 -9 | TMSI                  | e4a6de94  | 65534 | Paging               |
| 728 -7 | Contention Resolution | e4a6de94  | 18444 | RRC Connection Setup |
| 728 -7 | Contention Resolution | d77f73db  | 18810 | RRC Connection Setup |
| 732 -9 | TMSI                  | f0a4dbf4  | 65534 | Paging               |
| 735 -9 | TMSI                  | c75fa1f3  | 65534 | Paging               |
| 741 -9 | TMSI                  | d79080ee  | 65534 | Paging               |
| 756 -9 | TMSI                  | e013aa7b  | 65534 | Paging               |
| 758 -9 | TMSI                  | e4b8a883  | 65534 | Paging               |
| 781 -9 | TMSI                  | ee62b5f9  | 65534 | Paging               |
| 785 -9 | TMSI                  | f75face4  | 65534 | Paging               |

# Sniff (wireshark, control traffic)

Wireshark interface showing a packet capture of LTE control traffic. The packet list displays a sequence of frames, with packet 1199 highlighted in blue. The packet details pane shows the structure of the RLC-LTE [DL] [AM] SRB:1 [DATA] (P) sn=1 frame, including context, AM header, sequence analysis, and PDCP-LTE details.

| No.  | Time     | Source | Destination | Protocol        | Length | Channel | Info                                                              | time delta |
|------|----------|--------|-------------|-----------------|--------|---------|-------------------------------------------------------------------|------------|
| 1186 | 2.844832 |        |             | MAC-LTE         | 160    |         | DL-SCH: (SFN=885 , SF=0) UEId=0 (Padding:remainder)               | 0.002731   |
| 1187 | 2.845319 |        |             | LTE RRC DL_SCH  | 41     |         | SystemInformationBlockType1                                       | 0.000487   |
| 1188 | 2.848659 |        |             | MAC-LTE         | 156    |         | DL-SCH: (SFN=885 , SF=2) UEId=0 (Padding:remainder)               | 0.003340   |
| 1189 | 2.848676 |        |             | MAC-LTE         | 88     |         | DL-SCH: (SFN=885 , SF=2) UEId=0 (Padding:remainder)               | 0.000017   |
| 1190 | 2.852355 |        |             | LTE RRC DL_DCCH | 60     |         |                                                                   | 0.003679   |
| 1191 | 2.852555 |        |             | RLC-LTE         | 37     |         | [DL] [AM] SRB:1 [CONTROL] ACK_SN=2                                | 0.000200   |
| 1192 | 2.866353 |        |             | RLC-LTE         | 41     |         | [DL] [AM] SRB:1 [CONTROL] ACK_SN=2                                | 0.013798   |
| 1193 | 2.871011 |        |             | MAC-LTE         | 228    |         | DL-SCH: (SFN=886 , SF=2) UEId=0 (Padding:remainder)               | 0.004658   |
| 1194 | 2.871030 |        |             | MAC-LTE         | 84     |         | DL-SCH: (SFN=886 , SF=2) UEId=0 (Padding:remainder)               | 0.000019   |
| 1195 | 2.871046 |        |             | LTE RRC DL_DCCH | 60     |         | [DL] [AM] SRB:1 [CONTROL] ACK_SN=3                                | 0.000016   |
| 1196 | 2.876811 |        |             | LTE RRC DL_DCCH | 106    |         | HandoverFromEUTRANPreparationRequest                              | 0.005765   |
| 1197 | 2.877079 |        |             | LTE RRC DL_SCH  | 41     |         | SystemInformationBlockType1                                       | 0.000268   |
| 1198 | 2.877540 |        |             | RLC-LTE         | 41     |         | [DL] [AM] SRB:1 [CONTROL] ACK_SN=3                                | 0.000461   |
| 1199 | 2.878985 |        |             | LTE RRC DL_DCCH | 84     |         | RRConnectionRelease                                               | 0.001445   |
| 1200 | 2.888022 |        |             | MAC-LTE         | 440    |         | DL-SCH: (SFN=887 , SF=4) UEId=0 (4:417 bytes) (Padding:remainder) | 0.009037   |

**RLC-LTE [DL] [AM] SRB:1 [DATA] (P) sn=1 [41-bytes]**

- [Context]
  - [Direction: Downlink (1)]
  - [RLC Mode: Acknowledged Mode (4)]
  - [Channel Type: SRB (4)]
  - [Channel ID: 1]
  - [PDU Length: 43]
  - [AM Sequence number length: 10]
- AM Header (P) sn=1
  - 1... .... = Frame type: Data PDU (0x1)
  - .0... .... = Re-segmentation Flag: AMD PDU (0x0)
  - ..1... .... = Polling Bit: Status report is requested (0x1)
  - ...0 0... = Framing Info: First byte begins a RLC SDU and last byte ends a RLC SDU (0x0)
  - .... .0... = Extension: Data field follows from the octet following the fixed part of the header (0x0)
  - .... ..00 0000 0001 = Sequence Number: 1
- [Sequence Analysis - SN 1 retransmitted]
  - [OK: False]
  - [Retransmitted frame: True]
    - [Expert Info (Warning/Sequence): AM Frame retransmitted for Downlink on UE 0 - most likely in response to NACK (SRB-1)]
    - [AM Frame retransmitted for Downlink on UE 0 - most likely in response to NACK (SRB-1)]
    - [Severity level: Warning]
    - [Group: Sequence]
- PDCP-LTE sn=1
  - [Configuration: (direction=Downlink, plane=Signalling)]
    - [Direction: Downlink (1)]
    - [Plane: Signalling (1)]
    - [Channel type: DCCH (1)]
    - [Channel Id: 1]
    - [ROHC Compression: False]
  - [UE Security (ciphering=EEA2, integrity=EIA2)]
    - [Configuration frame: 1171]
    - [Ciphering Algorithm: EEA2 (2)]
    - [Integrity Algorithm: EIA2 (2)]
    - 000. .... = Reserved: 0
    - ...0 0001 = Seq Num: 1

# Sniff (RNTI, TMSI, modulace 3)

- **RNTI** a **TMSI** by měli být dočasné random identifikátory
- lze ale korelovat i sledovat polohu telefonu
- **RRC Connection setup/release** byl příklad, kdy telefon nemá security context
  - bude vysvětleno dále

# IMSI jde v plaintextu

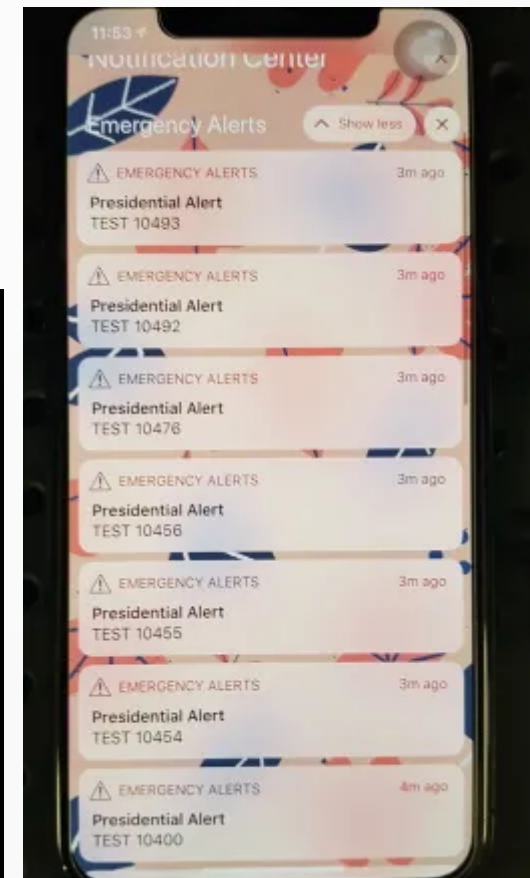
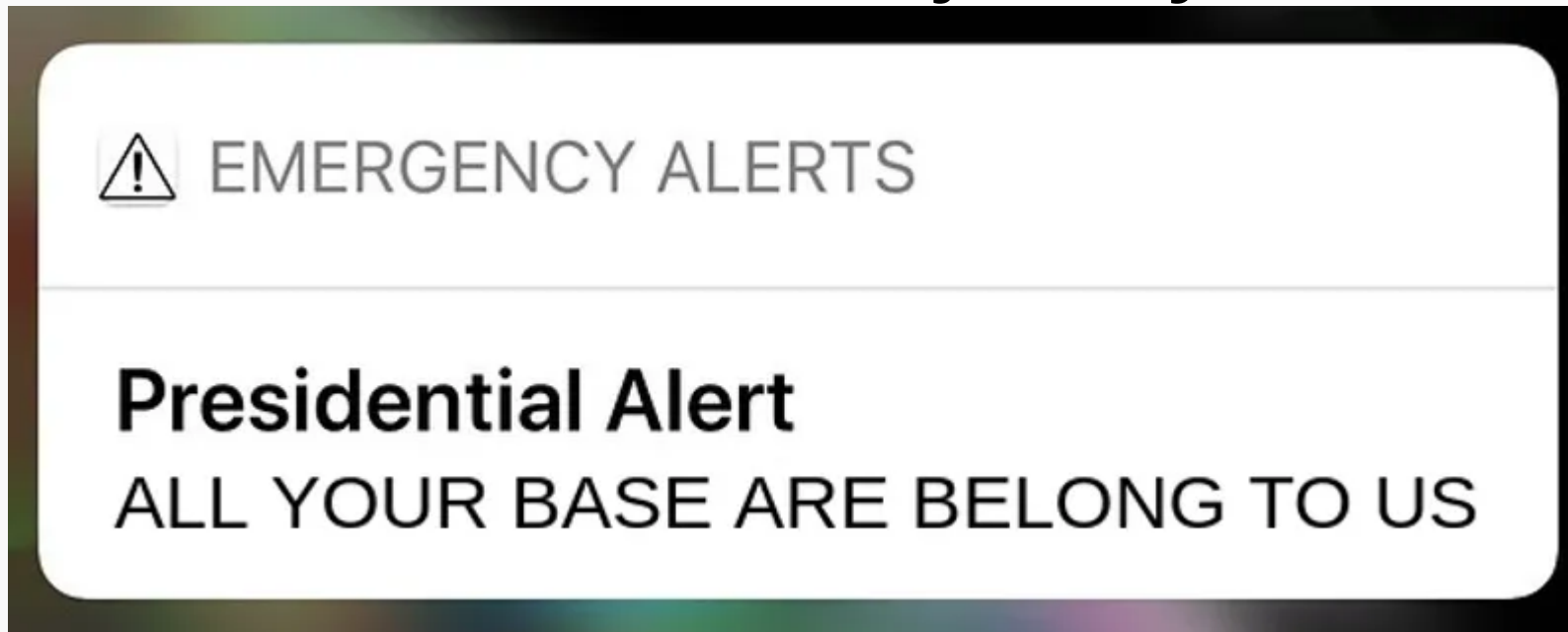
- Na začátku **telefon pošle svůj IMSI v plaintextu**
  - stačí poslouchat RRC Release
  - když mění bejsku např
  - nebo aktivní útok – nastavit pár parametrů, frekvenci a výkon
- Fejkovat lze než od eNB přijde **SecurityMode command**
  - tam **lze vypnout šifrování** z fake bejsky ale **ne integritu**
  - tudíž bez klíče smůla, neprojde bez integrity SecurityMode
  - modulo mnoho chyb protokolu

# Stav “bez security contextu” (1)

- Když telefon mění bejsky (RRC Release), tak je bez **security contextu**
- Lze počkat nebo různě vynutit
  - mnoho paperů, někdy šílený timing na subframech
- Aktivním zarušením “neighbor eNB” nastane downgrade na 3G, pak 2G (modulo implementace)
- 3G A5/3 Kasumi i 2G A5/1 lze cracknout rychle

# Stav “bez security contextu” (2)

- Bez security contextu lze některé zprávy pustit do UE
  - bez autentizace a autorizace
  - pokusy o lokalizaci a další útoky
- “Presidential alert” (CMAS) je nevyšší



# Sniff od “oktáfky vedle baráku”

- Útočník musí mít klíče od operátora, aby dal SecurityMode
- Nebo downgradovat na 3G a zlomit Kasumi
- Obě řešení se komerčně prodávají
  - blackboxy jak 1 m<sup>3</sup> kráva, ani ne sférická vo vakuu (cca víme jak fungují)
    - barevně černé, chtělo by je to barevně ještě černější, minimálně VantaBlack černé
  - antény lze ale dát na střechu osobáku jako takovou placku, aby to nebylo jen tak vidět, od antény a síly signálu závisí mnoho
- Je mnoho dalších útoků než jen “poslouchat”
  - napojit na exploity, AES-CTR bitflip...

# 5G

- 5G je cca final\_final\_7.exe dokončeno
  - 4G je taky dost guláš.png.exe v detailech, not final
- 5G má úplně jinou strukturu identit
  - SUPI - Subscription Permanent Identifier (IMSI ekvivalent)
    - může být ve vzduchu v plaintextu, i kdyby nemělo (scheme 0)
  - SUCI - Subscription Concealed Identifier (dočasná identita)
    - založeno na eliptických křivkách – ECIES s Curve25519 resp secp256r1
  - GUTI - Globally Unique Temporary UE Identity
    - periodicky se mění

# 5G...

- 5G má “standalone” a “non-standalone” mod
- non-standalone je kvůli rozšiřování z 4G na 5G postupně
  - hackish, nalepení na síťovou vrstvu
- tudíž různé útoky, ale můžou být sdíleny někdy
- vendor i prodával box na MitM (detaily nepamatuju)

# 2G po 5G

## Porovnání bezpečnostních prvků generací mobilních sítí

| Bezpečnostní prvky / mobilní technologie     | 2G  | 3G        | 4G        | 5G  |
|----------------------------------------------|-----|-----------|-----------|-----|
| Ověřování účastníka / zařízení v síti        | Ano | Ano       | Ano       | Ano |
| Síťové ověřování zařízení / účastníka        | Ne  | Ano       | Ano       | Ano |
| Ověřování propojení mezi operátory           | Ne  | Ne        | Ne        | Ano |
| Šifrování IPSec                              | Ne  | Volitelně | Volitelně | Ano |
| Integrita dat konec – konec                  | Ne  | Ne        | Ne        | Ano |
| Šifrování dat konec – konec                  | Ne  | Ne        | Ne        | Ano |
| Funkce skrytí identity účastníka (SUCI/SUPI) | Ne  | Ne        | Ne        | Ano |

**Telco sítě jsou MEGA BORDEL. FIN.**