2018
Arab Security Conference
المؤتمر العربي لأمن المعلومات

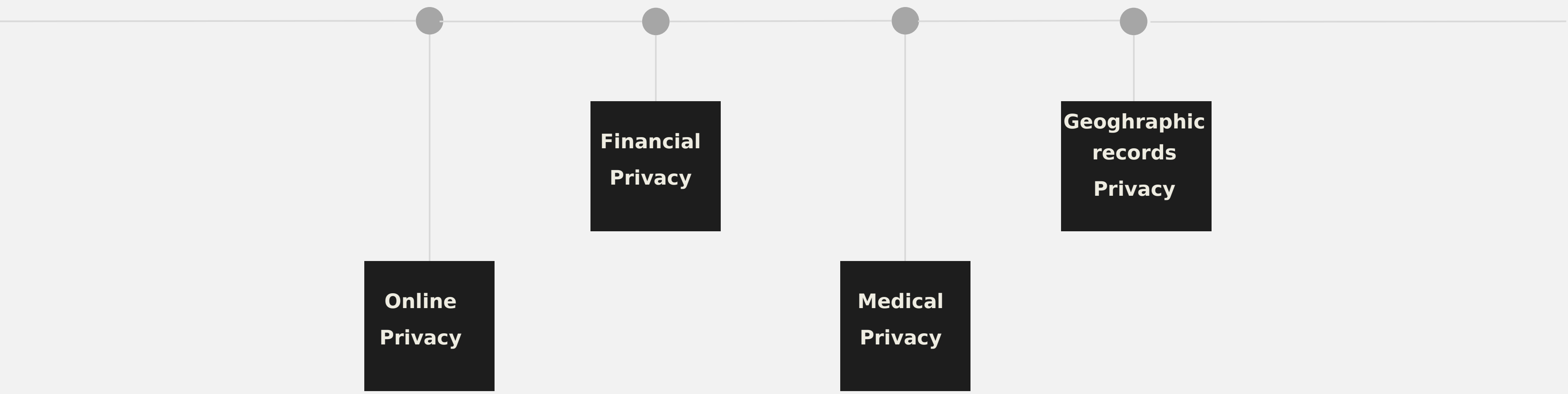
User Privacy on GSM Broadcast Channels

Loay Abdelrazek,
Security Researcher
Nile University

CYBER WARGAMES
Arab Security Championship 2018

Data Privacy

What type of data to be included ?



Can it be applied to telecom ?

Data Privacy

Problems with providing Data Security

Difficulty in understanding and defining what is sensitive data and what is not.

Difficulty in understanding and defining what is sensitive data and what is not.

Difficulty in understanding and defining what is sensitive data and what is not.

Thus, We need a broader definition…

Data Privacy

Any personal data that could be sensitive or can be used maliciously by someone and has a severe impact is included when considering data privacy.

Agenda

GSM Architecture

Network Components.
Subscriber Identities.
GSM Logical Channels.

Sniffing your traffic

Passive Sniffing Vs Active Sniffing.
Passive IMSI Catching.

Impact of Identity Leakage

Why its important to hide subscriber’s identites.
Demo.

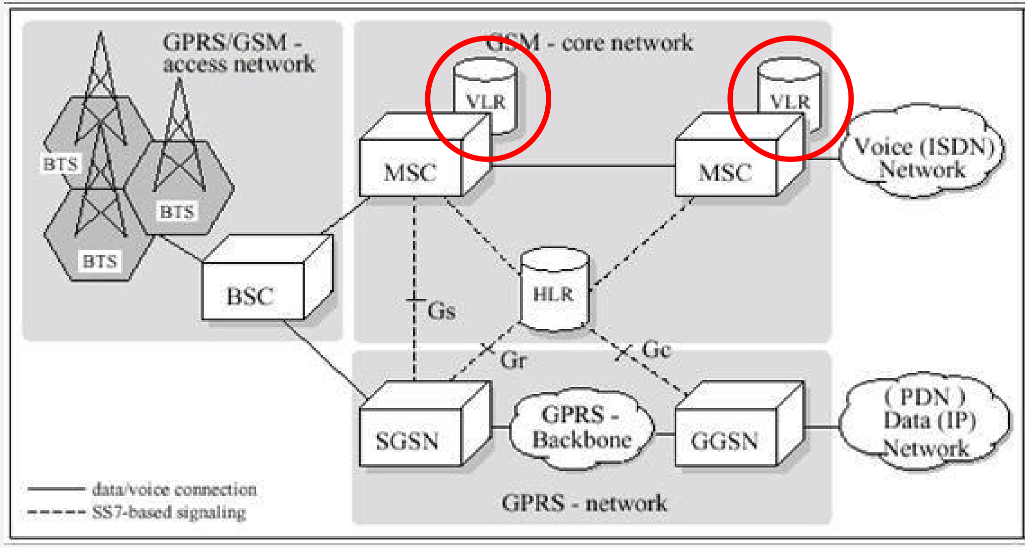
? Q&A

GSM Architecture

Network Components

Visitor Location Register (VLR)

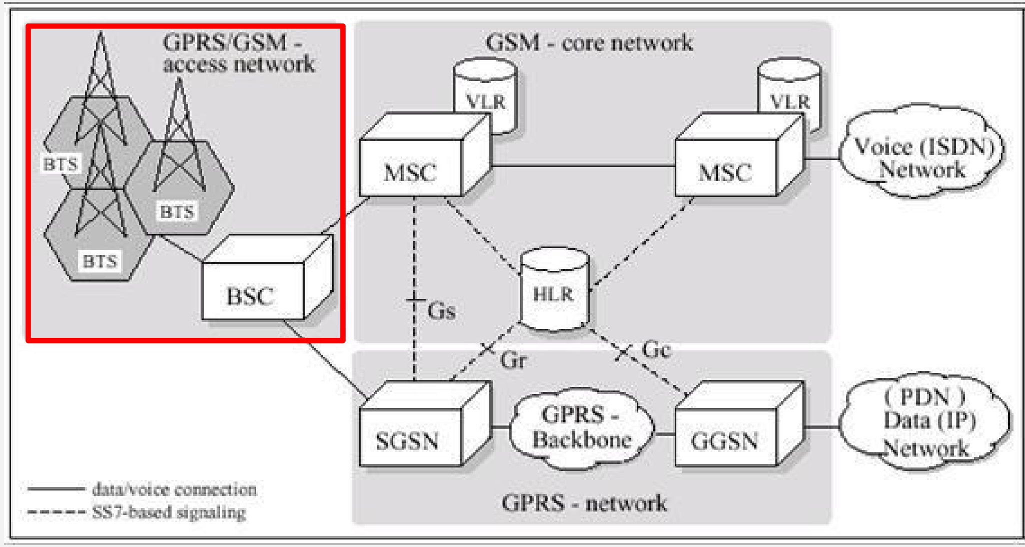
A mobile subscriber roaming in a network area covered by a mobile switching center is controlled by a VLR. The VLR is responsible of the authentication and registration procedures for mobile subscribers, upon updating its location to a new location area controlled by a VLR. The VLR also generates and handles the temporary IDs (TMSI) of the mobile subscribers in its area.



Network Components

The Base Station System (BSS)

The network of base station equipment composed of base station transceivers (BTS), and base station controllers (BSC). BSS is responsible of communicating with a mobile subscriber in a certain area.

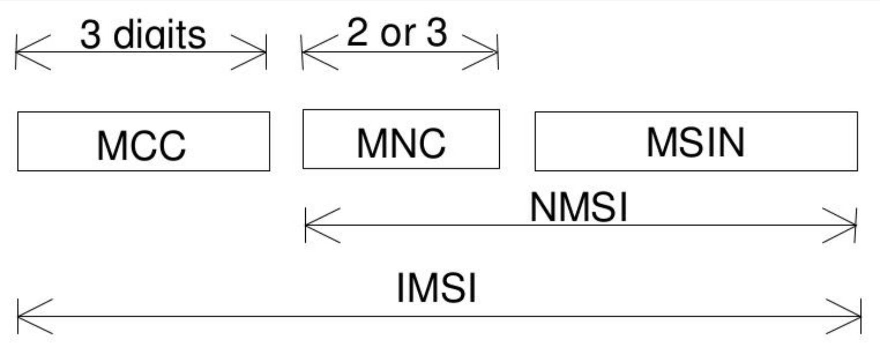


Subscriber Identities

International Mobile Subscriber Identity – IMSI

The IMSI is the main identifier in mobile networks and belongs to one specific SIM card. It is a 15 digit number where the first three digits identify the home country (MCC, Mobile Country Code), the following two or three digits identify the home network (MNC, Mobile Network Code). The remaining digits identify the specific user/SIM within the provider’s database .

The main usage for IMSI, is authentication, access provisioning and accounting.

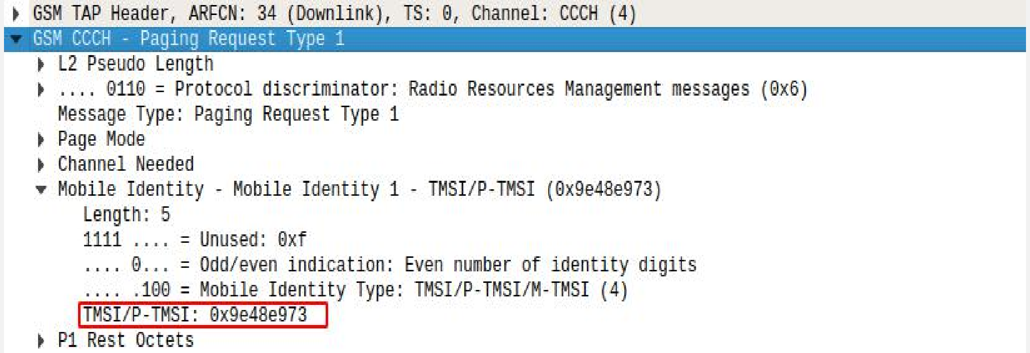


Subscriber Identities

Temporary Mobile Subscriber Identity – TMSI

The TMSI aims to protect subscribers’ confidentiality. The TMSI is a temporary identifier provided to the mobile device by the VLR, to be used instead of the IMSI. The TMSI has only local significance within a VLR and area controlled by a VLR.

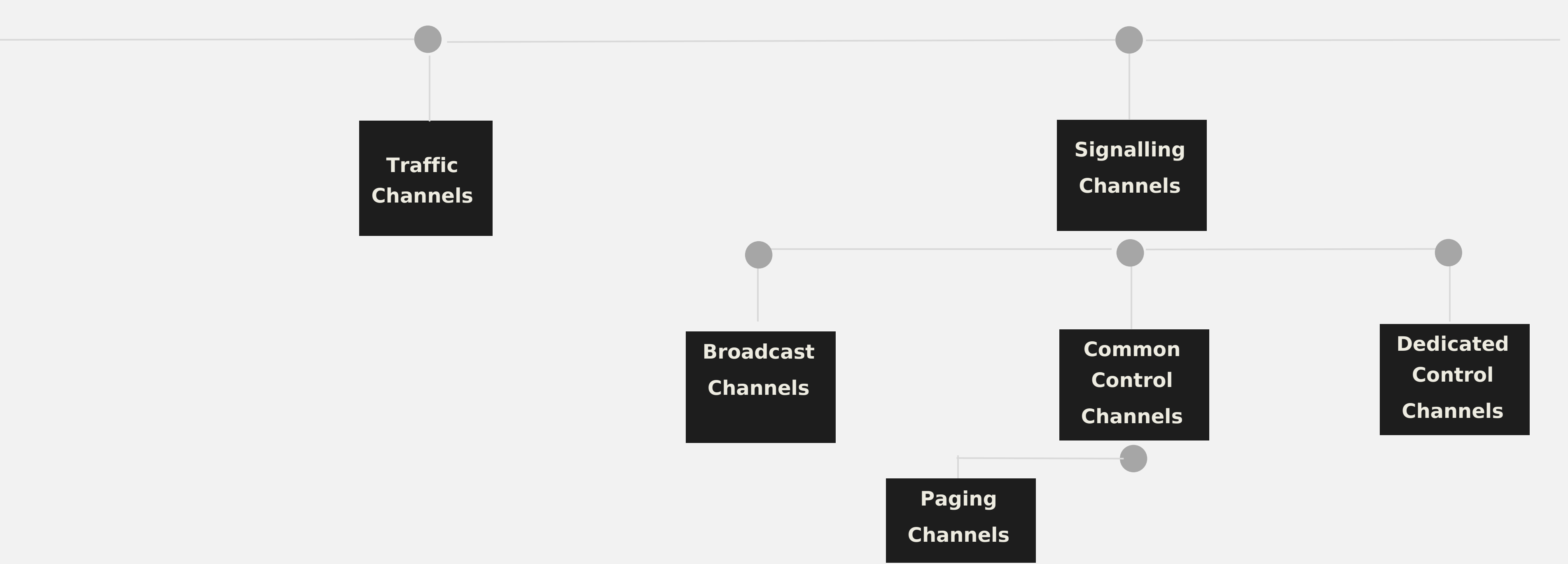
TMSI essentially masks the IMSI against passive attacks…All communication between mobile station and the network should be with TMSI and not IMSI



```
▸ GSM TAP Header, ARFCN: 34 (Downlink), TS: 0, Channel: CCCH (4)
▾ GSM CCCH - Paging Request Type 1
  ▸ L2 Pseudo Length
  ▸ .... 0110 = Protocol discriminator: Radio Resources Management messages (0x6)
    Message Type: Paging Request Type 1
  ▸ Page Mode
  ▸ Channel Needed
  ▾ Mobile Identity - Mobile Identity 1 - TMSI/P-TMSI (0x9e48e973)
      Length: 5
      1111 .... = Unused: 0xf
      .... 0... = Odd/even indication: Even number of identity digits
      .... .100 = Mobile Identity Type: TMSI/P-TMSI/M-TMSI (4)
      TMSI/P-TMSI: 0x9e48e973
  ▸ P1 Rest Octets
```

The TMSI is composed of 4 **bytes**, and represented in hexadecimal format as the following example: **“0x9e48e973“**

Logical Channels



Traffic Channels

Signalling Channels

Broadcast Channels

Common Control Channels

Dedicated Control Channels

Paging Channels

Logical Channels

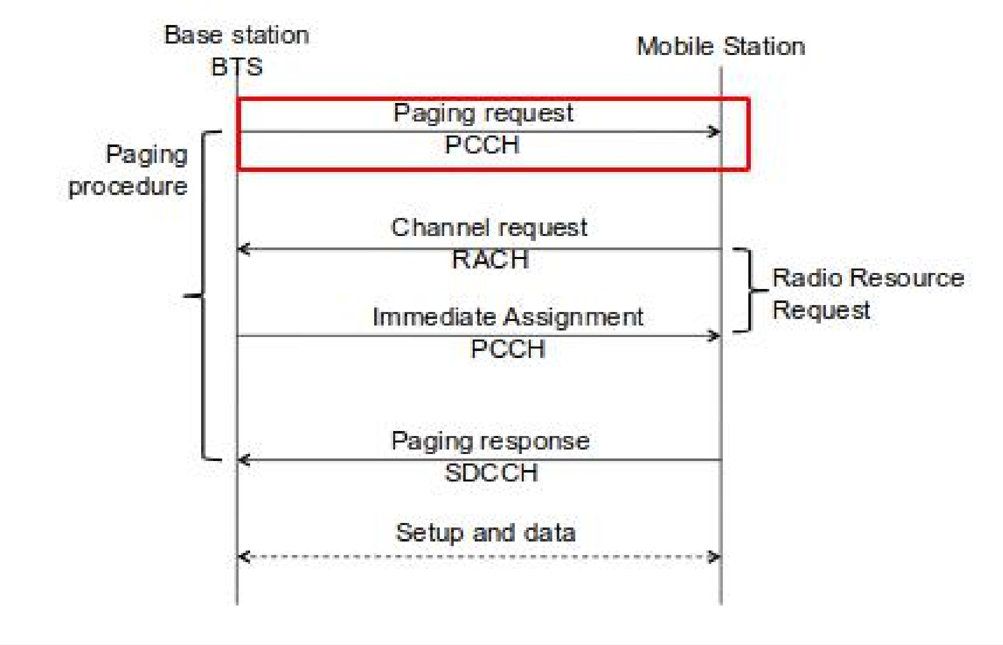
Common Control Channels (CCCH):

A group of uplink and downlink channels between the MS and the BTS. These channels are used to convey information from the network to MSs and provide access to the network. The CCCHs include the following channels.

Paging Channels (PCH):

Is a downlink sub-channel of the CCCH. PCH is used for paging of mobile subscribers upon receiving a sms or a call. All mobile stations can listen to this channel, and based on the identity sent on this channel a MS will respond.

Paging Requests



Sniffing Your Traffic

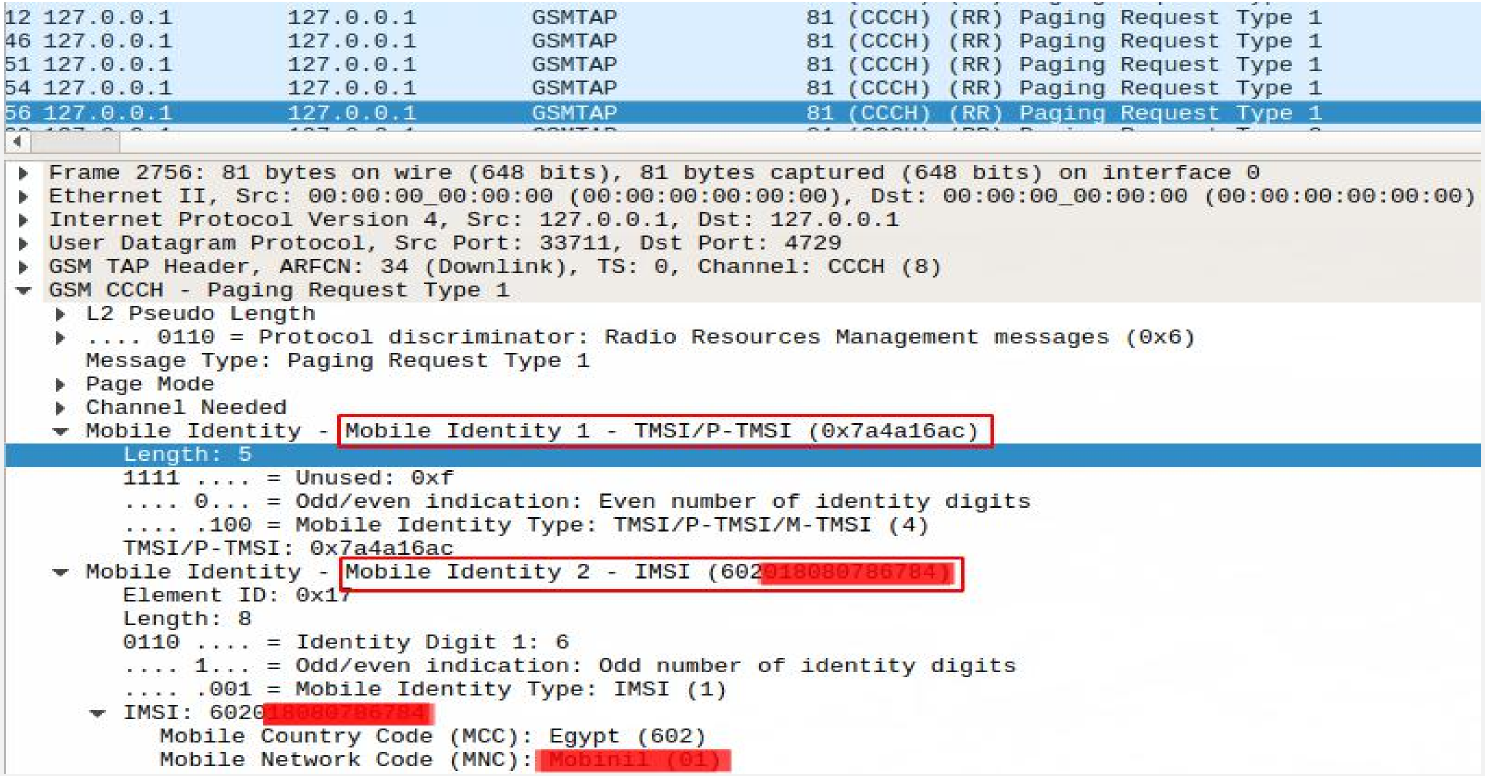
Passive Sniffing

Tuning to a specific frequency

Depending on the HW you can listen to GSM bands, UMTS or LTE.

This technique is of high risk. Its deployment is fairly easy.

Demo – Passive IMSI Catching



```
12 127.0.0.1        127.0.0.1        GSMTAP          81 (CCCH) (RR) Paging Request Type 1
46 127.0.0.1        127.0.0.1        GSMTAP          81 (CCCH) (RR) Paging Request Type 1
51 127.0.0.1        127.0.0.1        GSMTAP          81 (CCCH) (RR) Paging Request Type 1
54 127.0.0.1        127.0.0.1        GSMTAP          81 (CCCH) (RR) Paging Request Type 1
56 127.0.0.1        127.0.0.1        GSMTAP          81 (CCCH) (RR) Paging Request Type 1
```

```
▶ Frame 2756: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▶ User Datagram Protocol, Src Port: 33711, Dst Port: 4729
▶ GSM TAP Header, ARFCN: 34 (Downlink), TS: 0, Channel: CCCH (8)
▼ GSM CCCH - Paging Request Type 1
    ▶ L2 Pseudo Length
    ▶ .... 0110 = Protocol discriminator: Radio Resources Management messages (0x6)
      Message Type: Paging Request Type 1
    ▶ Page Mode
    ▶ Channel Needed
    ▼ Mobile Identity - Mobile Identity 1 - TMSI/P-TMSI (0x7a4a16ac)
          Length: 5
          1111 .... = Unused: 0xf
          .... 0... = Odd/even indication: Even number of identity digits
          .... .100 = Mobile Identity Type: TMSI/P-TMSI/M-TMSI (4)
          TMSI/P-TMSI: 0x7a4a16ac
    ▼ Mobile Identity - Mobile Identity 2 - IMSI (602[redacted]
          Element ID: 0x17
          Length: 8
          0110 .... = Identity Digit 1: 6
          .... 1... = Odd/even indication: Odd number of identity digits
          .... .001 = Mobile Identity Type: IMSI (1)
        ▼ IMSI: 6020[redacted]
              Mobile Country Code (MCC): Egypt (602)
              Mobile Network Code (MNC): [redacted]
```

Impact of Identity Leakage

Attack Scenario

Decrypting Voice/SMS traffic from air interface

An essential requirement to achieve this attack scenario is to retrieve the session key (Kc) used to decrypt the running session.

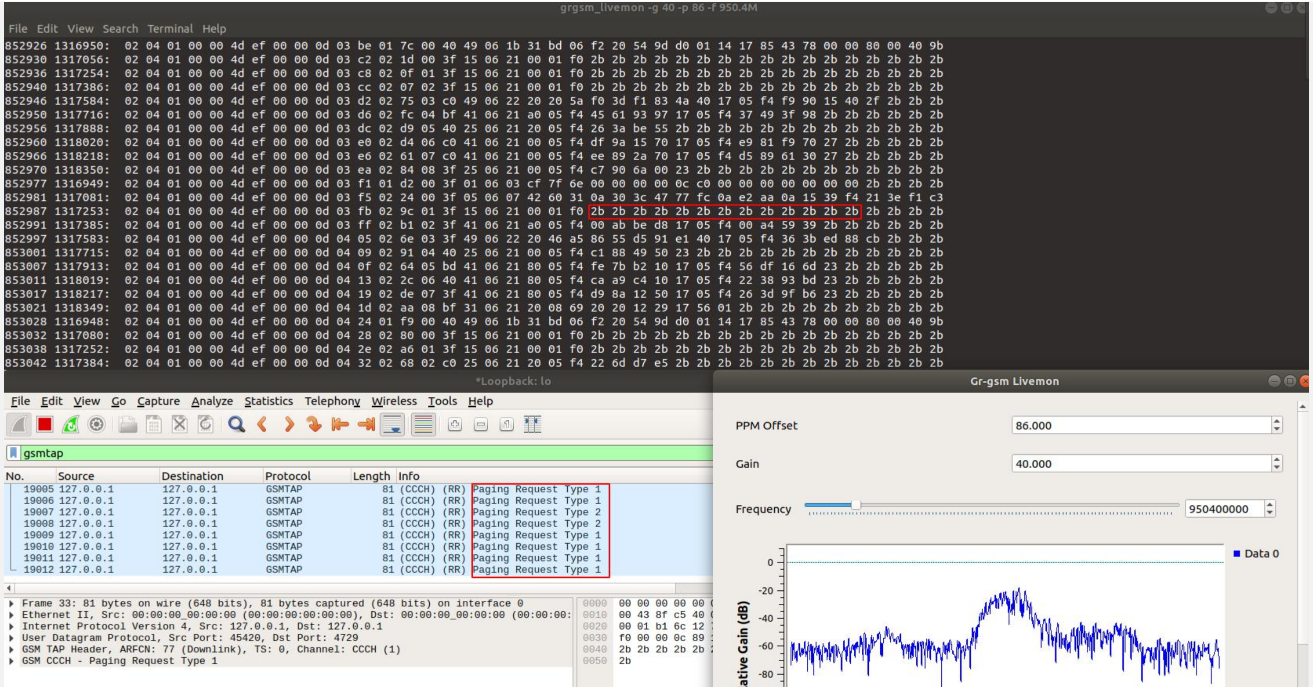
Retrieveing Kc is dependent on finding the ***IMSI***.

Attack Scenario

Decrypting Voice/SMS traffic from air interface

Sniffing for GSM traffic

‘2b‘ is padding byte for GSM



grgsm_livemon -g 40 -p 86 -f 950.4M

```
852926 1316950:  02 04 01 00 00 4d ef 00 00 0d 03 be 01 7c 00 40 49 06 1b 31 bd 06 f2 20 54 9d d0 01 14 17 85 43 78 00 00 80 00 40 9b
852930 1317056:  02 04 01 00 00 4d ef 00 00 0d 03 c2 02 1d 00 3f 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
852936 1317254:  02 04 01 00 00 4d ef 00 00 0d 03 c8 02 0f 01 3f 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
852940 1317386:  02 04 01 00 00 4d ef 00 00 0d 03 cc 02 07 02 3f 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
852946 1317584:  02 04 01 00 00 4d ef 00 00 0d 03 d2 02 75 03 c0 49 06 22 20 20 5a f0 3d f1 83 4a 40 17 05 f4 f9 90 15 40 2f 2b 2b 2b
852950 1317716:  02 04 01 00 00 4d ef 00 00 0d 03 d6 02 fc 04 bf 41 06 21 a0 05 f4 45 61 93 97 17 05 f4 37 49 3f 98 2b 2b 2b 2b 2b 2b
852956 1317888:  02 04 01 00 00 4d ef 00 00 0d 03 dc 02 d9 05 40 25 06 21 20 05 f4 26 3a be 55 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
852960 1318020:  02 04 01 00 00 4d ef 00 00 0d 03 e0 02 d4 06 c0 41 06 21 00 05 f4 df 9a 15 70 17 05 f4 e9 81 f9 70 27 2b 2b 2b 2b 2b
852966 1318218:  02 04 01 00 00 4d ef 00 00 0d 03 e6 02 61 07 c0 41 06 21 00 05 f4 ee 89 2a 70 17 05 f4 d5 89 61 30 27 2b 2b 2b 2b 2b
852970 1318350:  02 04 01 00 00 4d ef 00 00 0d 03 ea 02 84 08 3f 25 06 21 00 05 f4 c7 90 6a 00 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
852977 1316949:  02 04 01 00 00 4d ef 00 00 0d 03 f1 01 d2 00 3f 01 06 03 cf 7f 6e 00 00 00 00 0c c0 00 00 00 00 00 00 00 2b 2b 2b 2b
852981 1317081:  02 04 01 00 00 4d ef 00 00 0d 03 f5 02 24 00 3f 05 06 07 42 60 31 0a 30 3c 47 77 fc 0a e2 aa 0a 15 39 f4 21 3e f1 c3
852987 1317253:  02 04 01 00 00 4d ef 00 00 0d 03 fb 02 9c 01 3f 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
852991 1317385:  02 04 01 00 00 4d ef 00 00 0d 03 ff 02 b1 02 3f 41 06 21 a0 05 f4 00 ab be d8 17 05 f4 00 a4 59 39 2b 2b 2b 2b 2b 2b
852997 1317583:  02 04 01 00 00 4d ef 00 00 0d 04 05 02 6e 03 3f 49 06 22 20 46 a5 86 55 d5 91 e1 40 17 05 f4 36 3b ed 88 cb 2b 2b 2b
853001 1317715:  02 04 01 00 00 4d ef 00 00 0d 04 09 02 91 04 40 25 06 21 00 05 f4 c1 88 49 50 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
853007 1317913:  02 04 01 00 00 4d ef 00 00 0d 04 0f 02 64 05 bd 41 06 21 80 05 f4 fe 7b b2 10 17 05 f4 56 df 16 6d 23 2b 2b 2b 2b 2b
853011 1318019:  02 04 01 00 00 4d ef 00 00 0d 04 13 02 2c 06 40 41 06 21 80 05 f4 ca a9 c4 10 17 05 f4 22 38 93 bd 23 2b 2b 2b 2b 2b
853017 1318217:  02 04 01 00 00 4d ef 00 00 0d 04 19 02 de 07 3f 41 06 21 80 05 f4 d9 8a 12 50 17 05 f4 26 3d 9f b6 23 2b 2b 2b 2b 2b
853021 1318349:  02 04 01 00 00 4d ef 00 00 0d 04 1d 02 aa 08 bf 31 06 21 20 08 69 20 20 12 29 17 56 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
853028 1316948:  02 04 01 00 00 4d ef 00 00 0d 04 24 01 f9 00 40 49 06 1b 31 bd 06 f2 20 54 9d d0 01 14 17 85 43 78 00 00 80 00 40 9b
853032 1317080:  02 04 01 00 00 4d ef 00 00 0d 04 28 02 80 00 3f 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
853038 1317252:  02 04 01 00 00 4d ef 00 00 0d 04 2e 02 a6 01 3f 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
853042 1317384:  02 04 01 00 00 4d ef 00 00 0d 04 32 02 68 02 c0 25 06 21 20 05 f4 22 6d d7 e5 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
```

*Loopback: lo

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

gsmtap

```
No.   Source     Destination  Protocol  Length Info
19005 127.0.0.1  127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1
19006 127.0.0.1  127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1
19007 127.0.0.1  127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 2
19008 127.0.0.1  127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 2
19009 127.0.0.1  127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1
19010 127.0.0.1  127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1
19011 127.0.0.1  127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1
19012 127.0.0.1  127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1
```

```
▸ Frame 33: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 45420, Dst Port: 4729
▸ GSM TAP Header, ARFCN: 77 (Downlink), TS: 0, Channel: CCCH (1)
▸ GSM CCCH - Paging Request Type 1
```

```
0000  00 00 00 00 00
0010  00 43 8f c5 40
0020  00 01 b1 6c 12
0030  f0 00 00 0c 89
0040  2b 2b 2b 2b 2b
0050  2b
```

Gr-gsm Livemon

PPM Offset 86.000

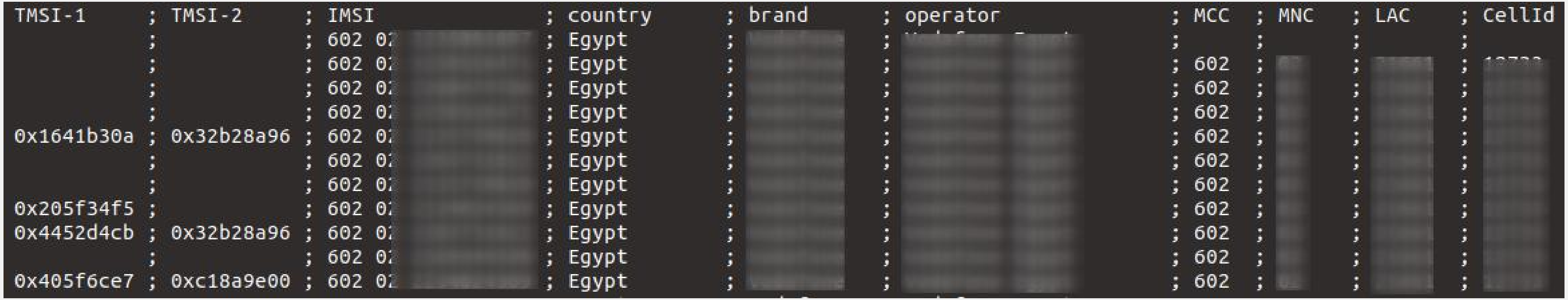
Gain 40.000

Frequency 950400000

Attack Scenario

Decrypting Voice/SMS traffic from air interface

Passive IMSI Catching technique to retrieve the IMSI of target.

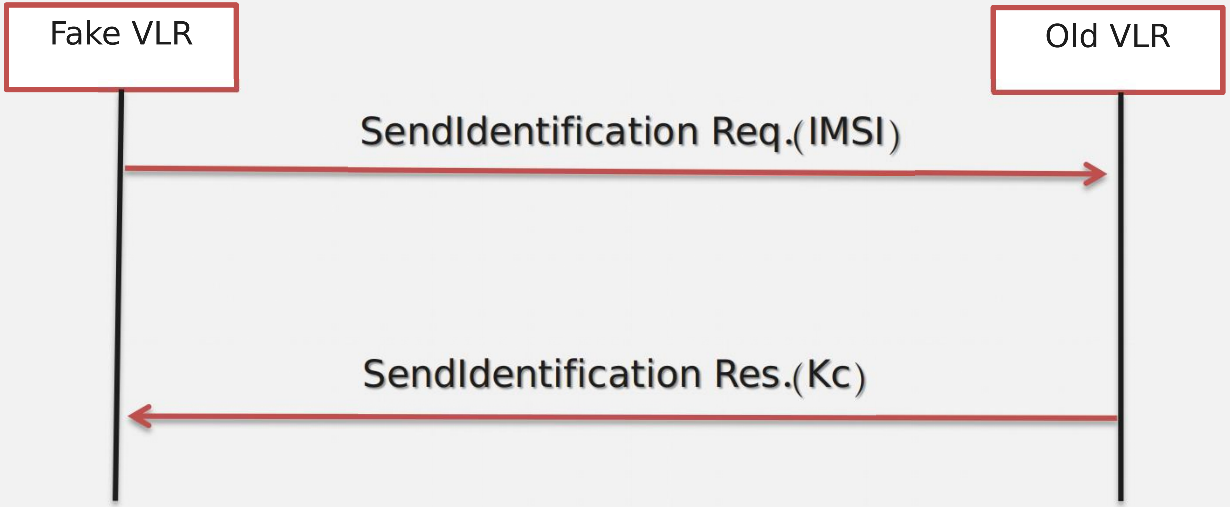


```
TMSI-1     ; TMSI-2     ; IMSI                ; country      ; brand      ; operator          ; MCC  ; MNC     ; LAC     ; CellId
           ;            ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ;      ;         ;         ;
           ;            ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ; 602  ; [redacted] ; [redacted] ; [redacted]
           ;            ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ; 602  ; [redacted] ; [redacted] ; [redacted]
           ;            ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ; 602  ; [redacted] ; [redacted] ; [redacted]
0x1641b30a ; 0x32b28a96 ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ; 602  ; [redacted] ; [redacted] ; [redacted]
           ;            ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ; 602  ; [redacted] ; [redacted] ; [redacted]
           ;            ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ; 602  ; [redacted] ; [redacted] ; [redacted]
0x205f34f5 ;            ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ; 602  ; [redacted] ; [redacted] ; [redacted]
0x4452d4cb ; 0x32b28a96 ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ; 602  ; [redacted] ; [redacted] ; [redacted]
           ;            ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ; 602  ; [redacted] ; [redacted] ; [redacted]
0x405f6ce7 ; 0xc18a9e00 ; 602 0[redacted]     ; Egypt        ; [redacted] ; [redacted]        ; 602  ; [redacted] ; [redacted] ; [redacted]
```

Attack Scenario

Decrypting Voice/SMS traffic from air interface

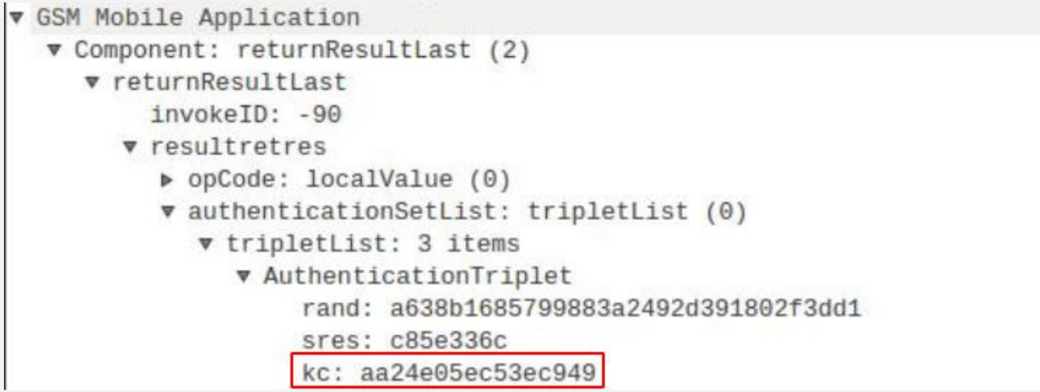
Remember SS7 ?



Attack Scenario

Decrypting Voice/SMS traffic from air interface

Retrieving Keys

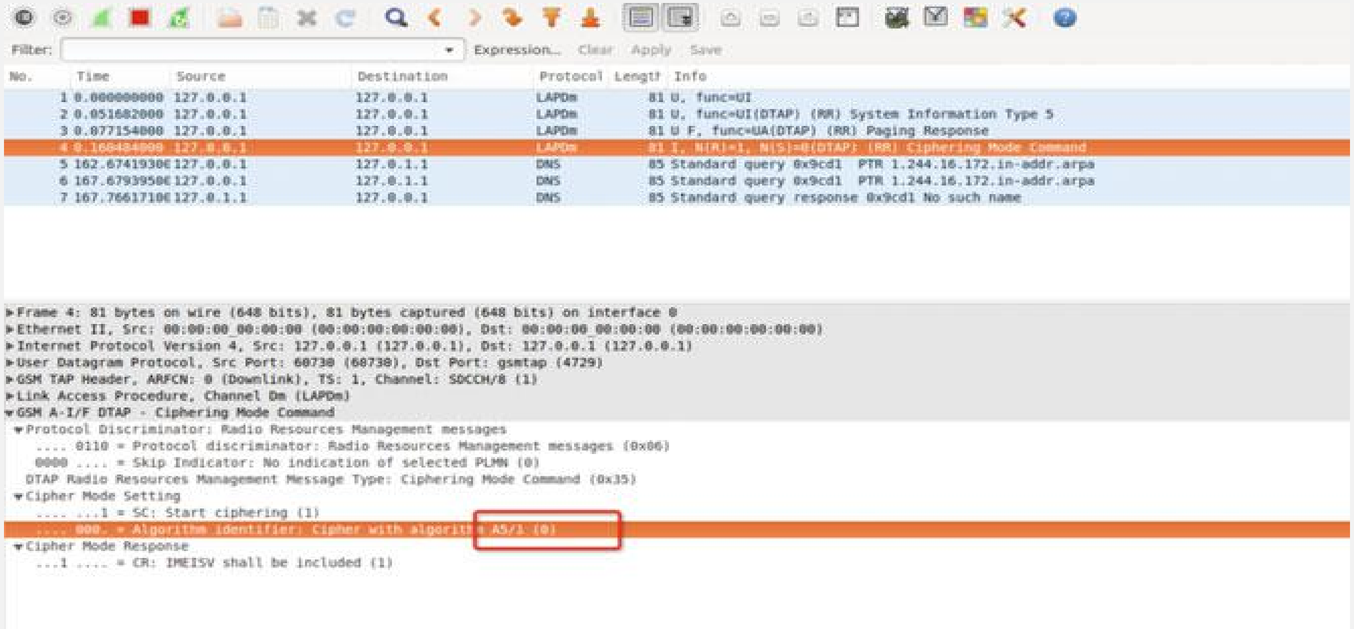


```
▼ GSM Mobile Application
  ▼ Component: returnResultLast (2)
    ▼ returnResultLast
        invokeID: -90
      ▼ resultretres
        ▶ opCode: localValue (0)
        ▼ authenticationSetList: tripletList (0)
          ▼ tripletList: 3 items
            ▼ AuthenticationTriplet
                rand: a638b1685799883a2492d391802f3dd1
                sres: c85e336c
                kc: aa24e05ec53ec949
```

Attack Scenario

Decrypting Voice/SMS traffic from air interface

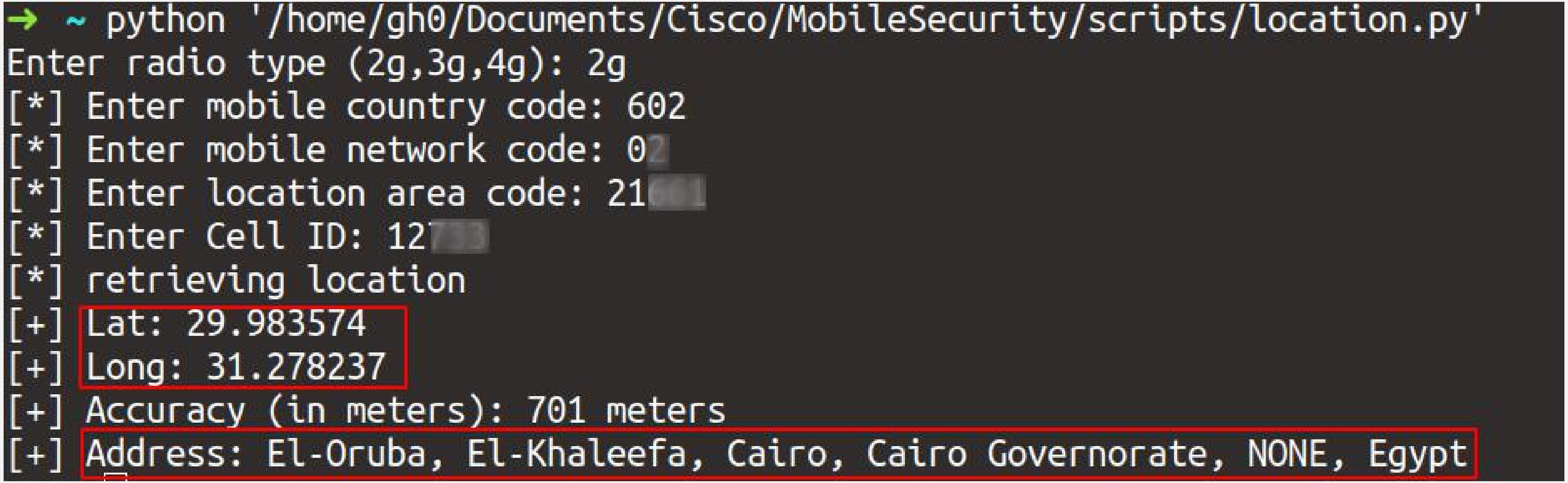
Detecting the ciphering algorithm used in this case its A5/1



```
No.    Time         Source      Destination  Protocol Lengtl Info
     1 0.000000000  127.0.0.1   127.0.0.1    LAPDm        81 U, func=UI
     2 0.051682000  127.0.0.1   127.0.0.1    LAPDm        81 U, func=UI(DTAP) (RR) System Information Type 5
     3 0.077154000  127.0.0.1   127.0.0.1    LAPDm        81 U F, func=UA(DTAP) (RR) Paging Response
     4 0.160484000  127.0.0.1   127.0.0.1    LAPDm        81 I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Command
     5 162.6741930€ 127.0.0.1   127.0.1.1    DNS          85 Standard query 0x9cd1  PTR 1.244.16.172.in-addr.arpa
     6 167.6793950€ 127.0.0.1   127.0.1.1    DNS          85 Standard query 0x9cd1  PTR 1.244.16.172.in-addr.arpa
     7 167.7661710€ 127.0.1.1   127.0.0.1    DNS          85 Standard query response 0x9cd1 No such name
```

```
▶Frame 4: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▶Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▶User Datagram Protocol, Src Port: 60738 (60738), Dst Port: gsmtap (4729)
▶GSM TAP Header, ARFCN: 0 (Downlink), TS: 1, Channel: SDCCH/8 (1)
▶Link Access Procedure, Channel Dm (LAPDm)
▼GSM A-I/F DTAP - Ciphering Mode Command
 ▼Protocol Discriminator: Radio Resources Management messages
   .... 0110 = Protocol discriminator: Radio Resources Management messages (0x06)
   0000 .... = Skip Indicator: No indication of selected PLMN (0)
  DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
 ▼Cipher Mode Setting
   .... ...1 = SC: Start ciphering (1)
   .... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)
 ▼Cipher Mode Response
   ...1 .... = CR: IMEISV shall be included (1)
```

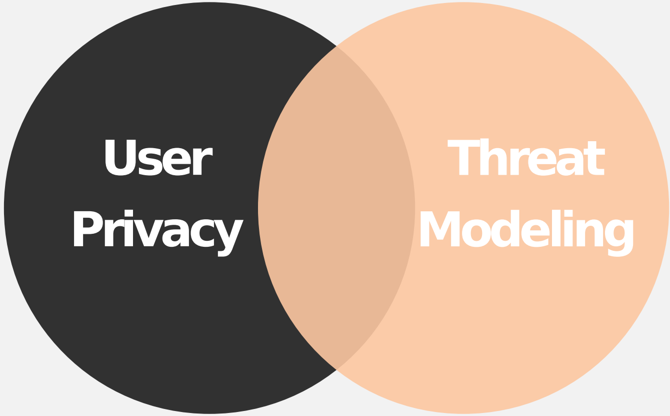
Attack Scenario



```
→ ~ python '/home/gh0/Documents/Cisco/MobileSecurity/scripts/location.py'
Enter radio type (2g,3g,4g): 2g
[*] Enter mobile country code: 602
[*] Enter mobile network code: 0[redacted]
[*] Enter location area code: 21[redacted]
[*] Enter Cell ID: 12[redacted]
[*] retrieving location
[+] Lat: 29.983574
[+] Long: 31.278237
[+] Accuracy (in meters): 701 meters
[+] Address: El-Oruba, El-Khaleefa, Cairo, Cairo Governorate, NONE, Egypt
```

Recommendations

Recommendations



User Privacy

Threat Modeling

Identify critical data.

Follow a correct threat modeling approach.

Configuration review.

Disable IMSI paging from core side (VLR and MME).

Reasonable refresh rate for session key (Kc).

? Q&A