

Mobile Security



Matej Kovačič
<https://pravokator.si>

Authentication problem

Mobile telephony does not have built-in proper authentication.

Caller or. SMS sender is “authenticated” only by his mobile number.

Result: Caller ID spoofing is possible!

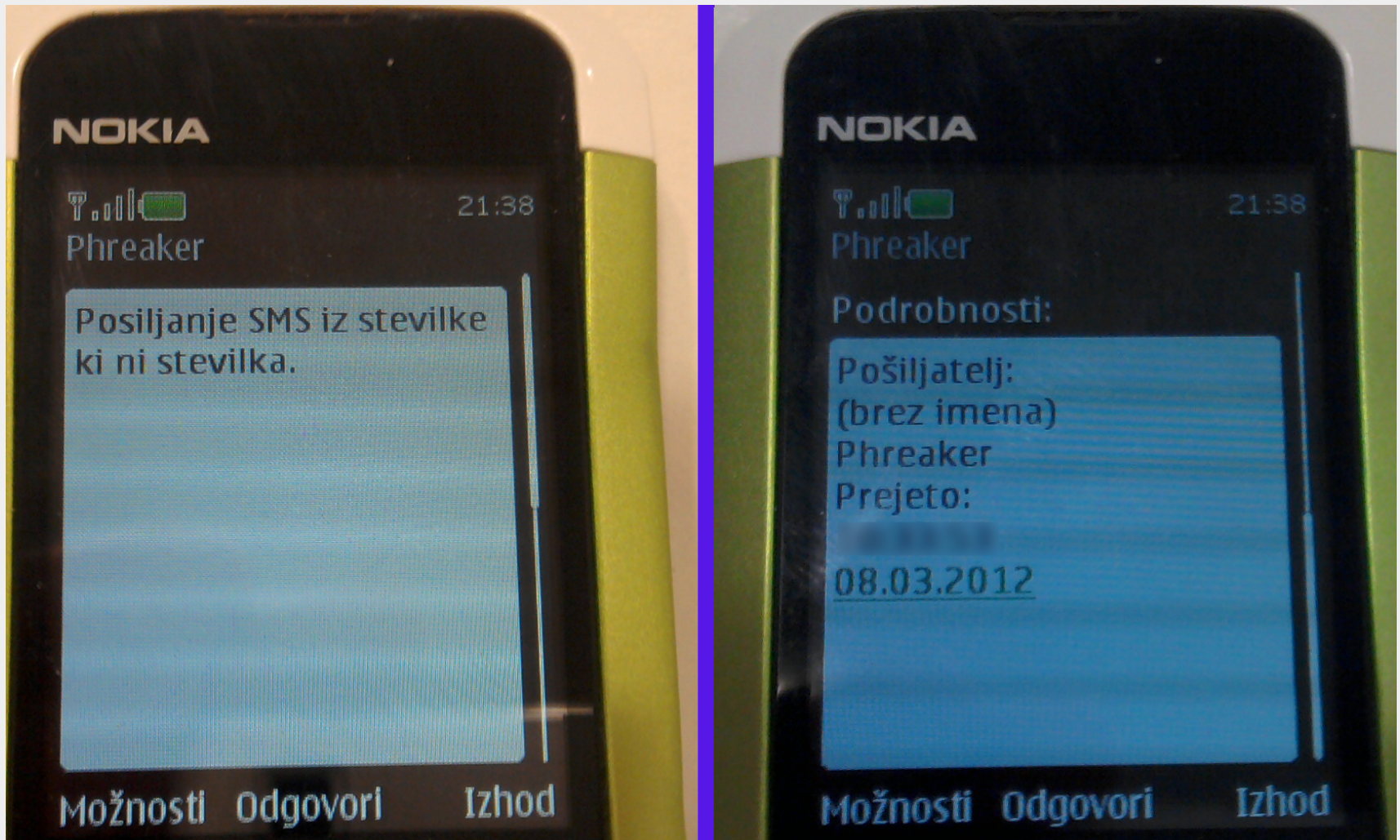
There is also lack of authentication among telecom providers.

Result: several possible attacks on SS7 infrastructure!

Mobile network is not authenticated to the mobile phone.

Result: fake base stations (i. e. IMSI catchers) could be used!

SMS spoofing



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

CallerID spoofing

trixbox - Admin Mode - Mozilla Firefox

192.168.56.101/maint/index.php?

trixbox CE
The Open Platform for Business Telephony

System Status Packages PBX System Settings

PBX Status: trixbox1.localdomain ()

Version
Asterisk 1.6.0.26-FONCORE-r78 built by...

Uptime
System uptime: 6 minutes, 9 seconds
Last reload: 6 minutes, 9 seconds

Active Channel(s)

Peer	User/ANR	Call
0	active SIP dialogs	

Sip Registry

Host	Username
sip.1000:5060	102
1 SIP registrations.	

Sip Peers

Name/username	Host
sip.1000:5060	102
2000	(Unspecified)
1000/1000	192.168.56.1
3 sip peers [Monitored: 0 online, 2 offline Unmonitored: 1 online, 0 offline]	

IAX2 Registry

Host	dnsmgr	Username	Perceived	Refresh	State
0 IAX2 registrations.					

IAX2 Peers

Name/Username	Host	Mask	Port	Status
0 iax2 peers [0 online, 0 offline, 0 unmonitored]				

```
trixbox1 login: root
Password:
Last login: Thu Feb  2 19:41:29 on tty1
trixbox1.localdomain ~# ifconfig tun0
tun0    Link encap:UNSPEC HWaddr 00-00-00-00-00-00
        inet addr:10.0.0.10  P-t-P:10.0.0.17  Mask:255.255.255.255
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
         RX packets:19 errors:0 dropped:0 overruns:0 frame:0
         TX packets:112 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:100
         RX bytes:10424 (10.1 KiB)  TX bytes:16714 (16.3 KiB)

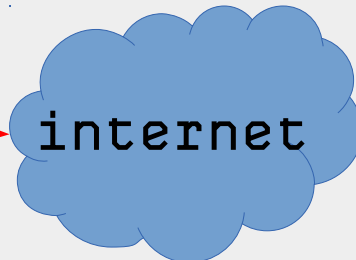
trixbox1.localdomain ~# _
```

SFLphone VoIP Client

38640

1 2 3
4 5 6
7 8 9
* 0 #

Using account TrixBox local (SIP)



VPN

4

3

1

2

CallerID spoofing

The image shows two overlapping browser windows displaying the Asterisk PBX administration interface. The background window shows the 'PBX Status' page with the following information:

- Version: Asterisk 1.6.0.26-FONCORE-r78 built by r
- 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]
- IAX2 Registry: 0 IAX2 registrations.
- IAX2 Peers: 1 iax2 peers [1 online, 0 offline, 0 unmonitored]

The foreground window shows the 'Extension: 1000' configuration page. A red arrow points to the 'Display Name' field, which contains the text 'Matej 1'. Other fields include 'CID Num Alias', 'SIP Alias', 'Outbound CID' (set to '386 [redacted] <386 [redacted]>'), 'Ring Time' (Default), 'Call Waiting' (Enable), and 'Call Screening' (Disable).

CallerID spoofing



CallerID spoofing

	25.02.2012	11:11:02	1 E	0	SVNSM-Si.mobil	SMS_poslan / 38631695xxx	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
					SVNSM-		

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

Practical use of spoofing :-)

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.

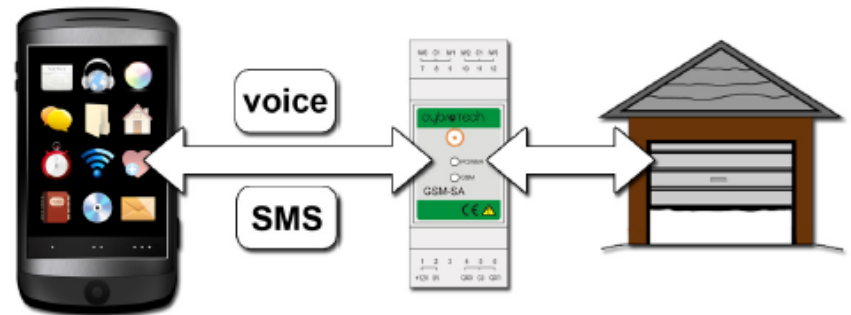
GSM module is a device which allows an authorized user to open or close the door. Device recognizes up to five specific phone numbers from which they can call on a GSM module which opens or closes the door.

Iku d.o.o. offers you:

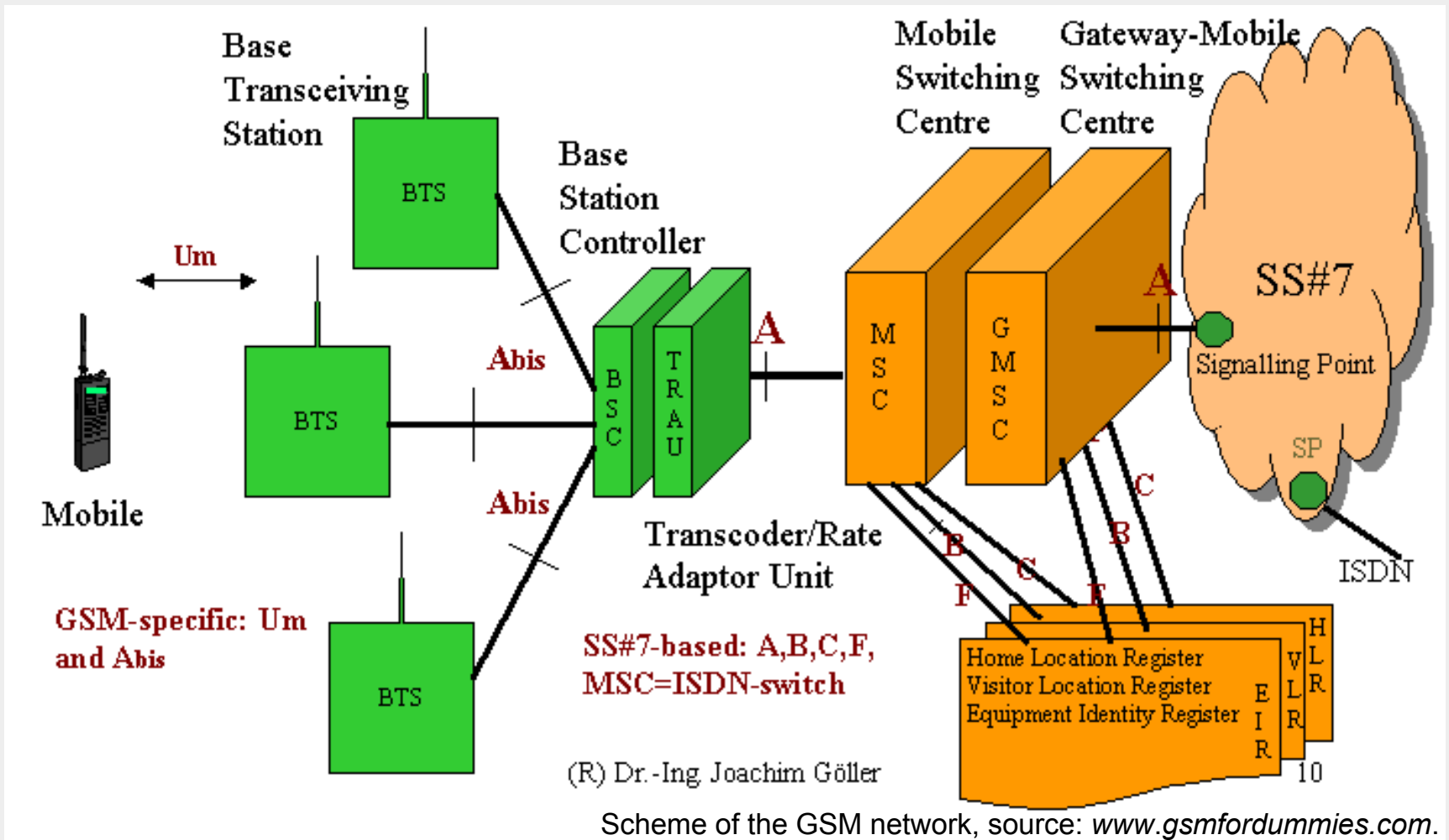
- delivery of a package with instructions for use,
- mounting points agreed upon (please call us and we will send you the offer).

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 additional equipment and appliances, because we assume that the mobile phone is already



Some GSM basics



SIM card and mobile equipment, IMSI, TMSI, A5/x, “broadcast channels” and data channels...

Capturing the signal in the past...



1 Use of phones with Calypso chipset...

```
matej@cryptopia: ~/osmocombb-raw/src/host/osmocon
Die ID code: 7e540b2fc90393bb
=====
REG_DPLL=0x2413
CNTL_ARM_CLK=0xf0a1
CNTL_CLK=0xff91
CNTL_RST=0xff3
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!
```

2 Connecting the phone to a computer with a special cable and loading modified ROM...

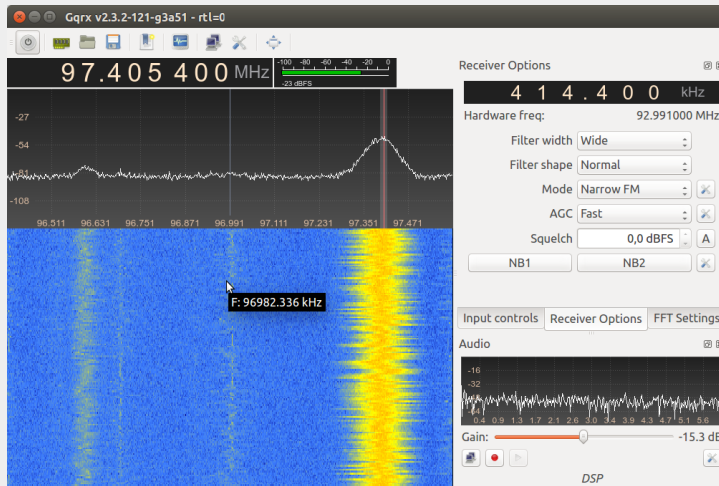
```
Failed to connect to '/tmp/osmocombb-raw/src/host/osmocon'.
Failed during sap.open(), no SIM reader
<000e> cell_log.c:803 Scanner initialized
Mobile initialized, please start phone now!
<000e> cell_log.c:367 Measure from 0 to 124
c<000e> cell_log.c:367 Measure from 512 to 885
<000e> cell_log.c:367 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, iPK0)
<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)
```

3 Running the applications for capture and analysis.

Capturing the signal today...



DVB-T device (with Elonics 4000 chipset; ~20 EUR).

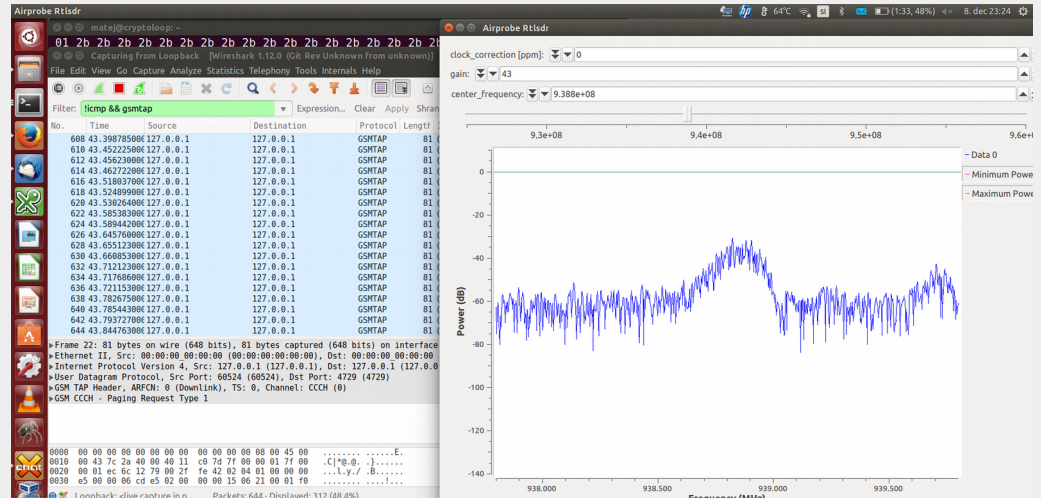
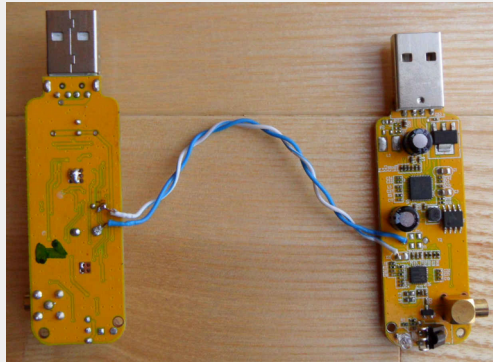


gr-gsm

Toolset for capture and analysis of GSM signals.

```
grgsm_livemon -p 35 -f 938.8M
```

```
wireshark -k -Y '!icmp && gsmtap' -i lo
```



```
grgsm_scanner -p 35
```

```
linux; GNU C++ version 4.9.1; Boost_105500; UHD_003.007.003-0-unknown
```

```
ARFCN: 18, Freq: 938.6M, CID: 0, LAC: 100, MCC: 293, MNC: 40, Pwr: -35  
ARFCN: 24, Freq: 939.8M, CID: 1313, LAC: 100, MCC: 293, MNC: 40, Pwr: -33  
ARFCN: 26, Freq: 940.2M, CID: 501, LAC: 100, MCC: 293, MNC: 40, Pwr: -27  
ARFCN: 124, Freq: 959.8M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -29
```

GSM security analysis in 2012

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 43 b7 81 40 00 40 11 85 26 7f 00 00 01 7f 00 C @ @ 8
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: ...

Some mobile operators were using A5/1 ciphering...

GSM security analysis in 2012

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: gsmmap Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
3825	68.987088000	127.0.0.1	127.0.0.1	GSM TAP	81	(CCCH) (RR) Paging Request Type 1
3826	69.013994000	127.0.0.1	127.0.0.1	GSM TAP	81	(CCCH) (RR) Paging Request Type 1
3827	69.033247000	127.0.0.1	127.0.0.1	GSM TAP	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... = SN capability (in SNs pt to pt capability): mobile station supports mobile terminated point to point SNs
... 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

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 supports A5/3...

GSM security analysis in 2012

The image shows a Wireshark 1.7.2 capture of GSM 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 2b ++++++ ++++++
0050 2b
```

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

GSM security analysis in 2012

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 3787 highlighted. The packet details pane shows the following structure:

- Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
- User Datagram Protocol, Src Port: 58444 (58444), Dst Port: gsmtap (4729)
- GSM TAP Header, ARFCN: 32 (Downlink), TS: 0, Channel: SDCCH/8 (5)
- Link Access Procedure, Channel Dm (LAPDm)
- ▼ GSM A-I/F DTAP - CIPHERING Mode Command
 - ▶ Protocol Discriminator: Radio Resources Management messages
 - DTAP Radio Resources Management Message Type: CIPHERING Mode Command (0x35)
 - ▼ Cipher Mode Setting
 -0 = SC: No ciphering (0)
 - ▼ Cipher Mode Response
 - ...1 = CR: IMEISV shall be included (1)

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

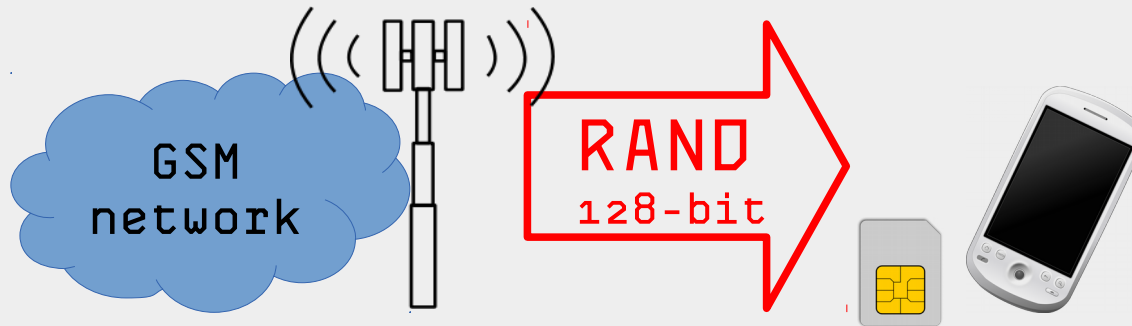
```
0010 00 43 4f b1 40 00 40 11 ec f6 7f 00 00 01 7f 00 .CO.@.@. ....
0020 00 01 e4 4c 12 79 00 2f fe 42 02 04 01 00 00 20 ...L.y./ .B....
0030 31 ff 00 19 7f 4b 08 00 05 00 03 00 0d 06 35 10 1....K.. .....5
0040 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b ++++++ ++++++
0050 2b +
```

In one network it was possible to switch off the encryption completely...

GSM encryption

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

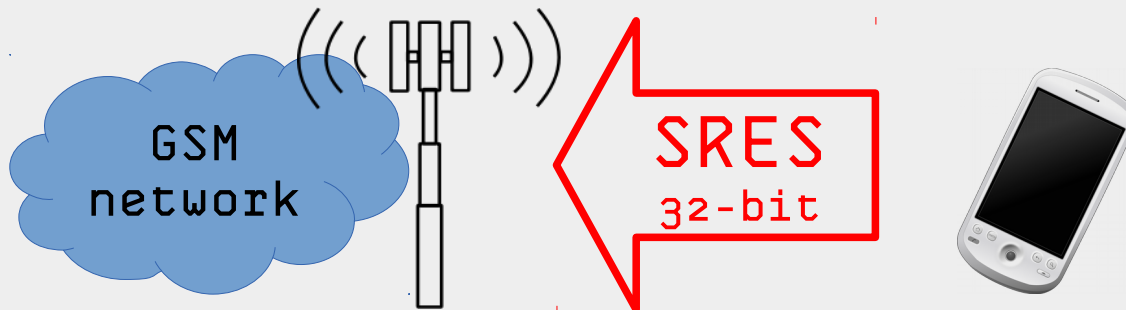
1.



HLR: $K_i + \text{RAND} @ A3 = \text{SRES}$

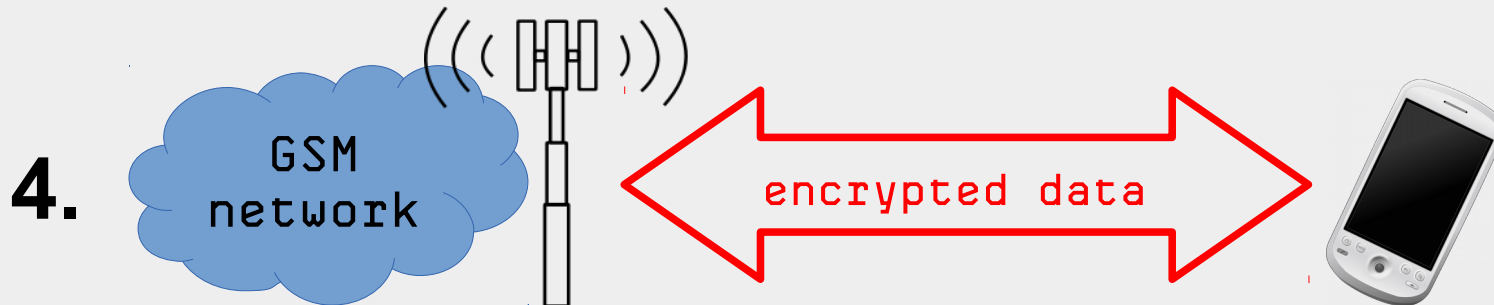
SIM card: $K_i + \text{RAND} @ A3 = \text{SRES}$

2.



GSM encryption

- 3.** On both sides K_c is created (with use of A8 algorithm):
 $K_i + \text{RAND} @ A8 = K_c$



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

GSM cryptanalysis

CONTENT OF DATA BURST IN GSM

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

"ONE-TIME" KEY FOR ENCRYPTION OF 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
----	----	----	----	----	----	----	----	----	----	----	----	----

$f(K_c)$



Kraken



K_c

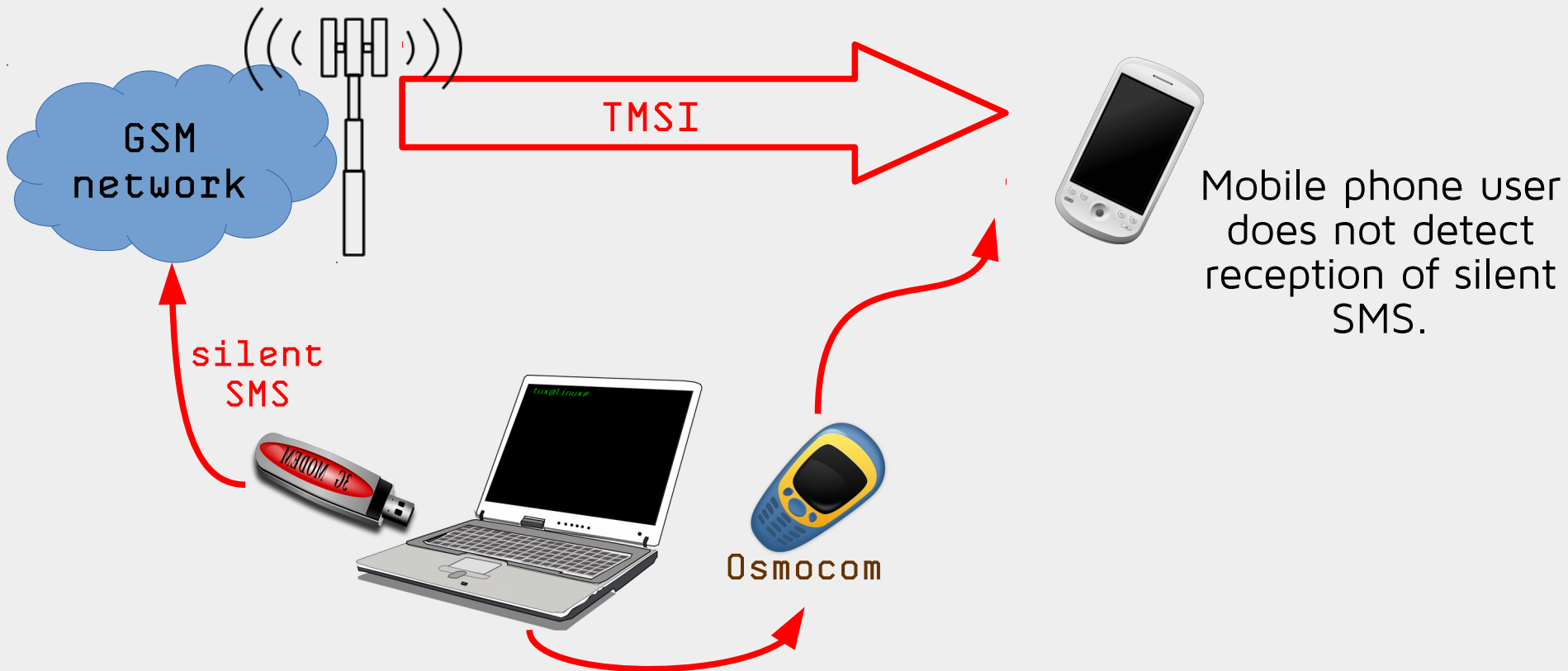
Random padding vs. non-random padding

```
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 0d 0d 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 +
```

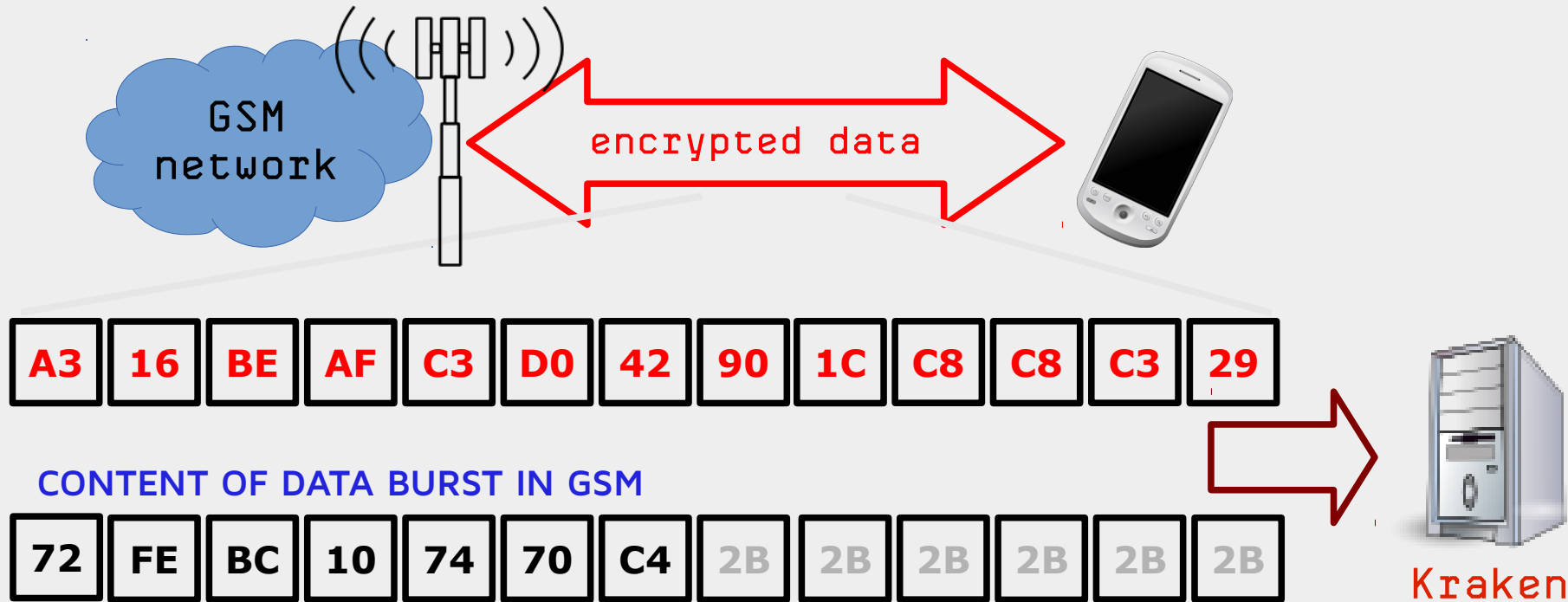
```
▼ GSM A-I/F DTAP - Identity Request
  ▶ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..01 1000 = DTAP Mobility Management Message Type: Identity Request (0x18)
    0000 .... = Spare bit(s): 0
  ▶ Identity Type
0020 00 01 0d 0d 12 79 00 21 1e 42 02 04 01 01 00 68 .....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 5d ]
```

Locating the 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.



Cryptanalysis in practice



- 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 K_c .
- In the process we need no access to the SIM card, mobile phone or mobile network!



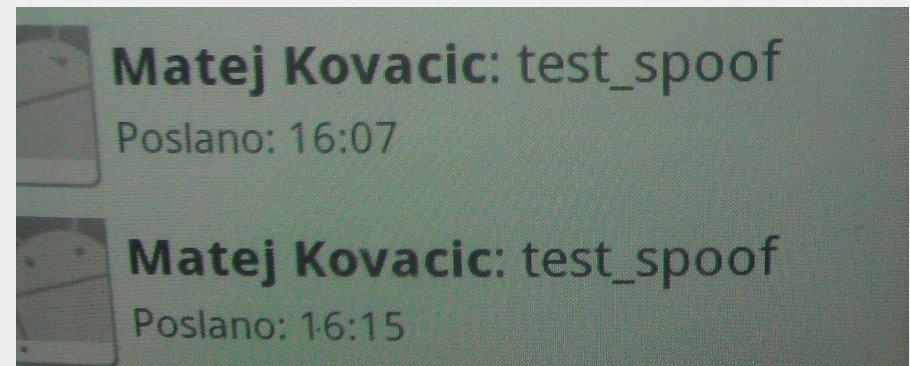
Mobile *identity* spoofing

For mobile **identity** spoofing we need:

- IMSI number (can get it via SS7 lookup),
- TMSI number (capture it from the network),
- session key (we crack it),
- key sequence number (capture it from the network).

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

```
matej@cryptopia: ~
matej@cryptopia: ~
testcard    Attach built in test SIM
spooft      Attach spoofing SIM
reader      Attach SIM from reader
remove      Detach SIM card
pin         Enter PIN for SIM card
disable-pin Disable PIN of SIM card
enable-pin  Enable PIN of SIM card
change-pin  Change PIN of SIM card
unblock-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
TMSI       TMSI you want to spoof
OsmocomBB# sim spoof 1 293
KC         Encryption key of spoofed mobile
OsmocomBB# sim spoof 1 293
KEY_SEQUENCE Key sequence
OsmocomBB# sim spoof 1 293
```



Two SMS messages sent by spoofed mobile identity.

IMSI Catchers

Basically, they are fake base stations



Alibaba.com Global trade starts here

Sourcing Solutions Services & Membership Help & Community

Categories Products What are you looking for... Search

About 2325 results: Other Telecommunications Products (47), VoIP Products (1694), Wireless Networking Equipment (408)

Home > Products > Telecommunications > Communication Equipment > Other Telecommunications Products (103492) [Subscribe to Trade Alert](#)

IMSI catcher

FOB Reference Price: [Get Latest Price](#)

US \$1,800 / Unit | 1 Unit/Units (Min. Order)

Contact Supplier

Leave Messages Add to My Cart

Payment: This supplier also supports Western Union payments for offline orders.

View larger image ZOOM

IMSI Catchers – how do they work?

First, they false introduce themselves as legitimate base station.

Then they report false Location Area code to the nearby mobile phones.

Now mobile phones are contact IMSI Catcher (Location Update), but with their TMSI number.

IMSI Catcher now false claims that mobile phone's TMSI has expired and requestts re-authentication.

Mobile phone now reports IMSI and IMEI number to IMSI Catcher.

IMSI Catcher now says it cannot accept a mobile phone (Location Update Reject), and redirects mobile phone back to the original operator.

Or not...

IMSI Catchers - can we detect them?

The image shows a Wireshark packet capture analysis. The top pane displays a list of packets, with packet 34 selected. The middle pane shows the packet details for the selected packet, and the bottom pane shows the raw packet bytes in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
24...	56.627398...	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 1
34...	81.125671...	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 1

Packet 34 details:

- User Datagram Protocol, Src Port: 57272, Dst Port: 4729
- GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: CCCH (5)
- GSM CCCH - Paging Request Type 1
 - L2 Pseudo Length
 - ... 0110 = Protocol discriminator: Radio Resources Management messages (0x6)
Message Type: Paging Request Type 1
 - Page Mode
 - Channel Needed
 - Mobile Identity - Mobile Identity 1 - IMSI ([REDACTED])
Length: 8
0010 = Identity Digit 1: 2
... 1... = Odd/even indication: Odd number of identity digits
... .001 = Mobile Identity Type: IMSI (1)
 - IMSI:** [REDACTED]
 - Mobile Country Code (MCC): Slovenia (293)
 - Mobile Network Code (MNC): SI Mobil (40)
 - P1 Rest Octets

Raw packet bytes (hex and ASCII):

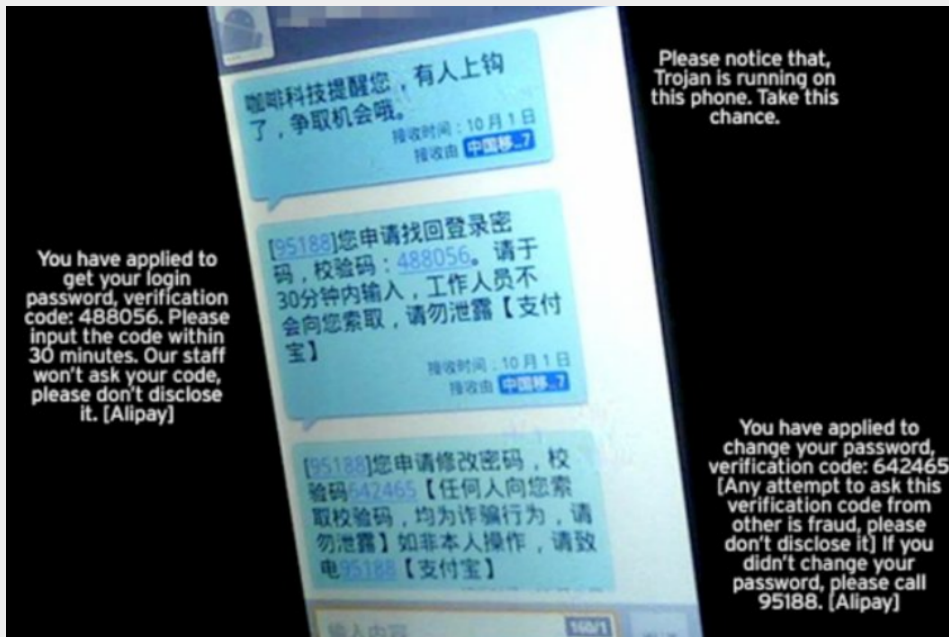
```
0010 00 43 70 31 40 00 40 11 cc 76 7f 00 00 01 7f 00 .Cp1@.@. .v.....
0020 [REDACTED] [REDACTED]
0030 [REDACTED] [REDACTED]
0040 [REDACTED] 2b 2b [REDACTED] +++++
0050 2b +
```

International mobile subscriber identity(IMSI) (e212.imsi), 8 bytes Packets: 4196 · Displayed: 2 (0.0%) · Load time: 0:0.83 Profile: Default

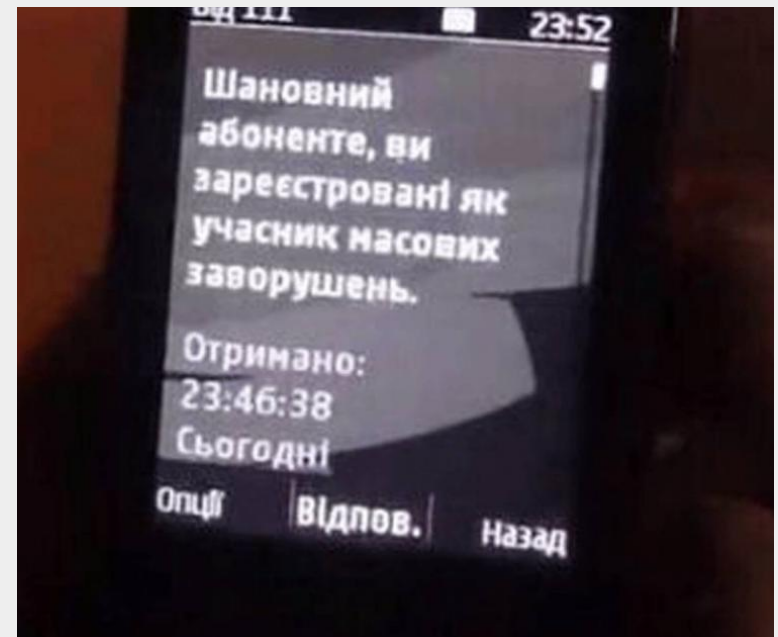
IMSI Catchers – what can they do?

IMSI Catcher can:

- **reveal the exact location** of a mobile phone,
- offer mobile phone a network connectivity and perform **MITM attack**,
- start calls and send SMS messages **past the network**.



Chinese SMS SPAM messages.

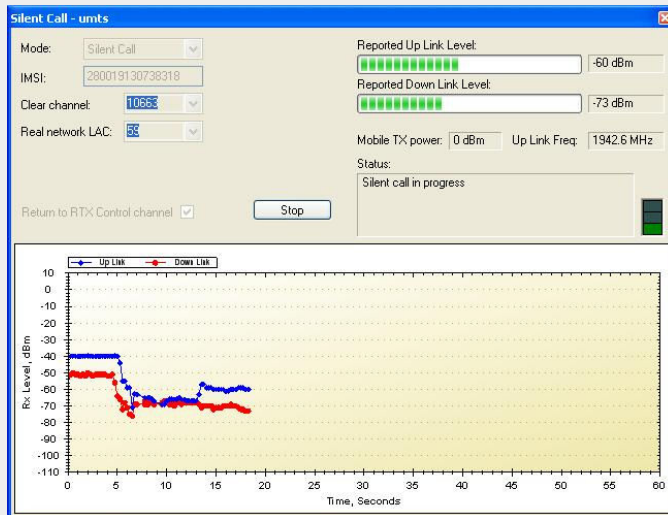


Ukraine – message to protestors.

IMSI Catchers – what can they do?

IMSI Catcher can also:

- **isolate** mobile phone from his network,
- **disable** the phone so it needs to be rebooted or **empty** his battery,
- performs a **silent call**, which opens the microphone and changes mobile phone to an eavesdropping device,
- **installs malware** via baseband attack.



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----- X

IN THE MATTER OF AN APPLICATION OF :
THE UNITED STATES OF AMERICA FOR :
AUTHORIZATION TO CONTINUE TO :
INTERCEPT ORAL COMMUNICATIONS :
OCCURRING AT (i) THE SEATING AREA :
INSIDE BRUNELLO TRATTORIA, 227 EAST :
MAIN STREET, NEW ROCHELLE, NEW YORK :
10801; (ii) THE SEATING AREA INSIDE :
MARIO'S RESTAURANT, 2342 ARTHUR :
AVENUE, BRONX, NEW YORK 10458; :
(iii) THE SEATING AREA INSIDE :
AGOSTINO'S RESTAURANT, 969 BOSTON :
POST ROAD, NEW ROCHELLE, NEW YORK :
10801; AND (iv) THE SEATING AREA :
INSIDE THE MARINA RESTAURANT, WRIGHT :
ISLAND MARINA 290 DRAKE AVENUE, NEW

APPLICATION FOR AN :
ORDER AUTHORIZING THE :
INTERCEPTION OF ORAL :
COMMUNICATIONS

Some SS7 attacks

Signalling System #7 is a protocol for exchanging data among telephone operators.

SS7 enables access to Home Location Register, Visitor Location Register and Mobile Switching Center...

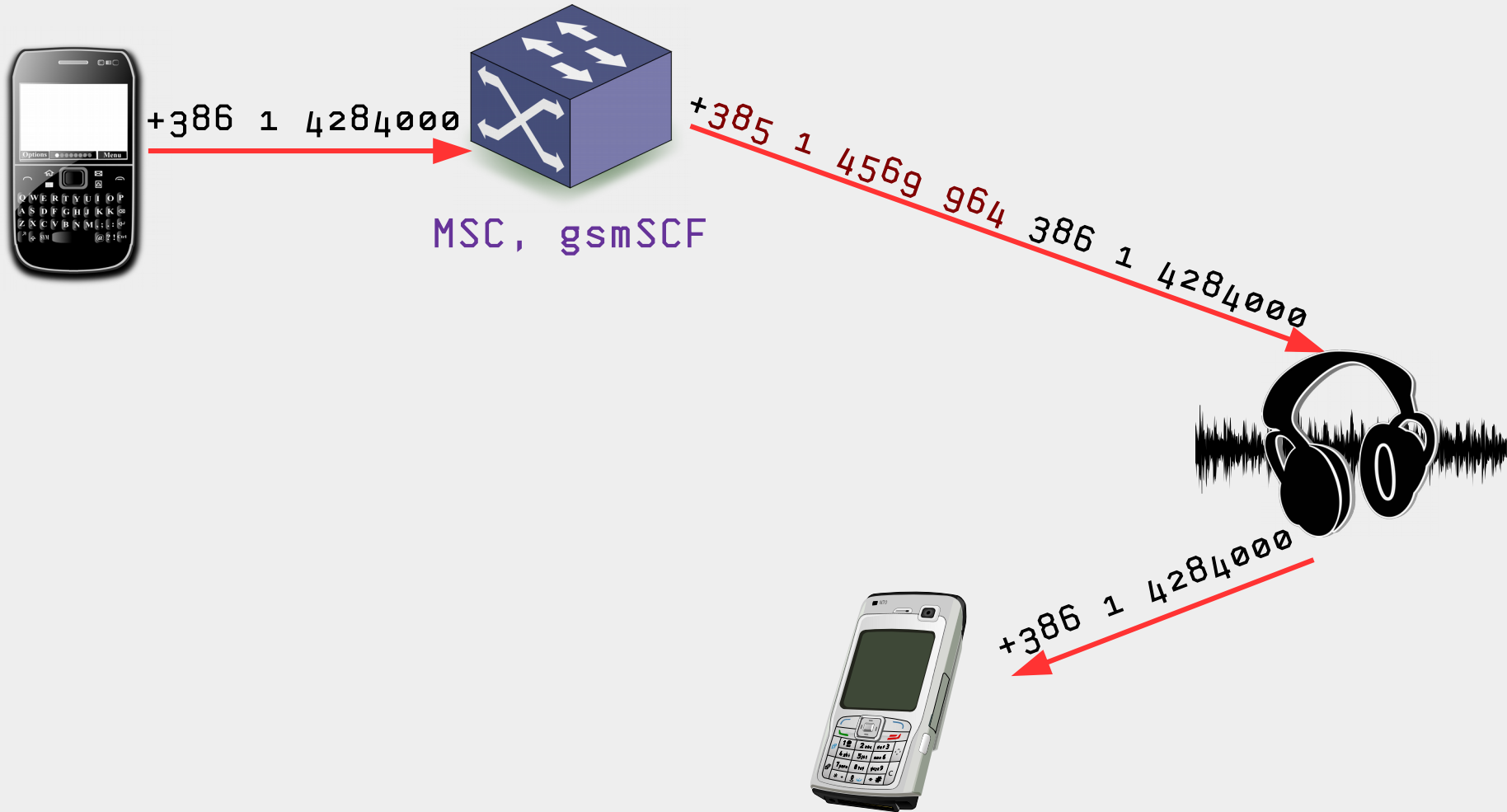
Since the authentication in SS7 is flawed, SS7 could bring us some fun...

Example: CAMEL (Customised Applications for Mobile networks Enhanced Logic) protocol abuse.

- User is roaming in some foreign network.
- User's local HLR tells roaming network's VLR that every time user wants to make a call, MSC should contact gsmSCF (GSM Service Control Function) in home network and ask what to do with a call.
- If user is calling "local number", gsmSCF rewrites number to international format (+386...) and tells MSC to continue with the new number.

Example: intercepting outgoing calls

...



Example: intercepting incoming calls

An attacker pretends that a subscriber is in his “network” by sending the *updateLocation* with his *Global Title* to the subscriber’s HLR.

All calls and SMS messages for that subscriber are now routed to the attacker.

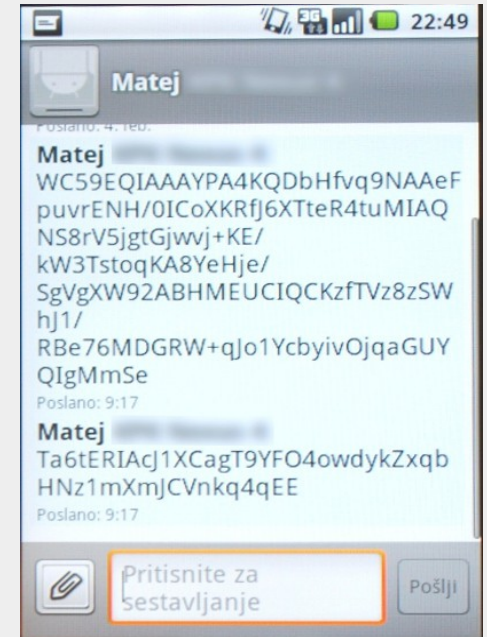
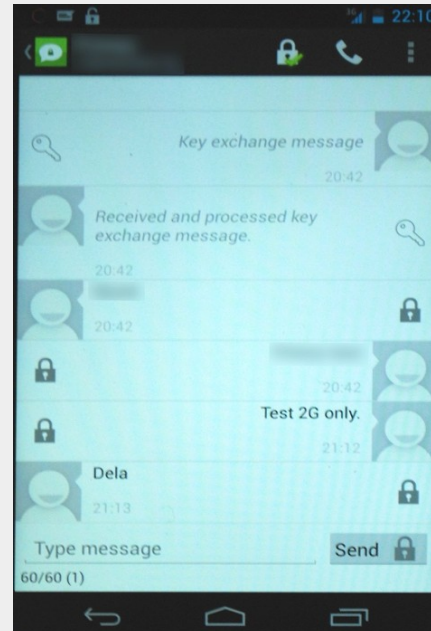
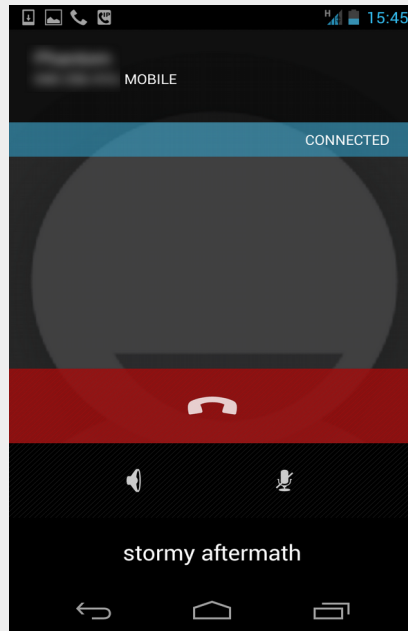
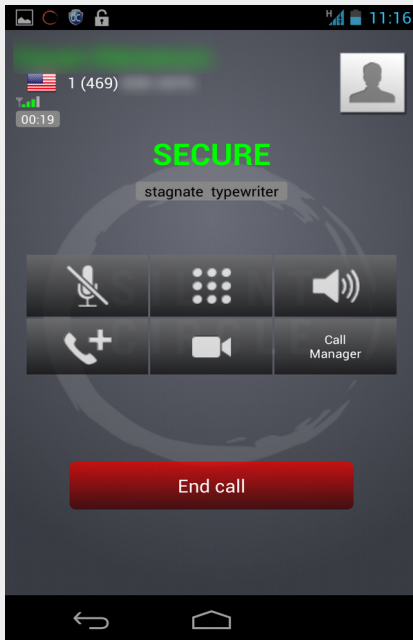
Now a victim logs into her/his bank account, and since s/he is using two-factor authentication, her/his bank sends SMS to her/his number with mTAN access code...

BUSTED!

Protection



Encryption of mobile communications



The main approach is to use data transfer and encryption on an application level.

Unencrypted vs. encrypted phone call

The image displays a network analysis setup for a VoIP call. The main window is Wireshark, showing a list of packets and a detailed view of SIP messages. A red box highlights the INVITE and ACK messages. Overlaid on this is a 'pcap - VoIP - RTP Player' window showing a waveform of the audio stream. A second window, 'encrypted_srtp_audio', shows the audio being played back, with a frequency of 44100 Hz. The RTP Player window also shows a 'Wrong Time' error for a packet drop.

Wireshark Packet List:

No.	Time	Source	Destination	Length	Protocol	Info
1	20:10:32.318				VoIP Calls	
2	20:10:32.318					
3	20:10:32.667					
4	20:10:32.669					
5	20:10:33.454					
6	20:10:33.454	21,162982	88,346119		SIP	<sip:031...@212.1
7	20:10:39.671	102,384695	160,364970	172.16.0.116	SIP	"Matej Kovacic" <sip:031...@212.1>
8	20:10:40.173					
9	20:10:41.175					
10	20:10:42.669					
11	20:10:42.671					
12	20:10:43.179					
13	20:10:47.665					
14	20:10:47.667					
15	20:10:50.715					
16	20:10:50.777					
17	20:10:52.669					
18	20:10:52.670					

Wireshark Packet Details:

- Message: PUBLISH sip:031...@212.1
- Message: INVITE sip:015805373@212.1, with
- Message: 100 Trying
- Message: ACK sip:015805373@212.1
- Message: INVITE sip:015805373@212.1 with
- Message: 100 Trying
- Message: 180 Ringing
- Message: CANCEL sip:015805373@212.1
- Message: 200 OK
- Message: 487 Request Cancelled
- Message: ACK sip:015805373@212.1

pcap - VoIP - RTP Player:

Start Time	Stop Time	Initial Speaker	From	To	Protoco	Packets	State	Comments
21,162982	88,346119		<sip:031...@212.1		SIP	7	COMPLETE	
102,384695	160,364970	172.16.0.116	"Matej Kovacic" <sip:031...@212.1>		SIP	14	COMPLETE	

encrypted_srtp_audio:

Frequency: 44100 Hz
Start: 00:00:00.000
End: 00:00:00.000

Signal application

There are several applications for encrypted mobile communications.

However, Signal app by Whisper Systems seems to be the best. On a technical level it has:

- strong encryption algorithms,
- perfect forward secrecy and future secrecy,
- detection of MITM attacks,
- »end-to-end« encryption,
- asynchronous communication,
- encrypted storage of messages.

Technical solution prevents eavesdropping on a communication link and by the operator.

Signal application

User level:

- easy to use,
- free of charge,
- source code is completely open,
- application has been security reviewed.



“ After reading the code, I literally discovered a line of drool running down my face. It’s really nice.

— **Matt Green**, Cryptographer, Johns Hopkins University



“ I am regularly impressed with the thought and care put into both the security and the usability of this app. It’s my first choice for an encrypted conversation.

— **Bruce Schneier**, internationally renowned security technologist

A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION SEARCH LANGUAGE MENU

SURVEILLANCE SELF-DEFENSE

Tips, Tools and How-tos for Safer Online Communications

Want a security starter pack?

Start from the beginning with a selection of simple steps.



“ Signal is the most scalable encryption tool we have. It is free and peer reviewed. I encourage people to use it everyday.

— **Laura Poitras**, Oscar winning filmmaker and journalist

Signal application

There are minimal traffic data logged.

Attachment A

<u>Account</u>	<u>Information</u>
[REDACTED]	N/A
[REDACTED]	Last connection date: [REDACTED] Unix millis Account created: [REDACTED] Unix millis

Signal could be further anonymized:

- by registering “unrelated phone number”,
- by using over Tor network,
- developers are building censorship circumvention into it.

Even NSA is »recommending« it! :-)

TOP SECRET//COMINT//REL FVEY//20340601

Capabilities Development Risk Matrix (II)

Impact > to production Use Risk v	TRIVIAL	MINOR	MODERATE	MAJOR	CATASTROPHIC
	Loss/lack of insight to small aspect of target communications, presence	Loss/lack of insight to significant aspect of target communications, presence	Loss/lack of insight to large component of target communications, presence	Loss/lack of insight to majority of target communications, presence	Near-total loss/lack of insight to target communications, presence
Current Highest Priority Target Use	Document tracking	Fivewes, Facebook chat presentation	Mail.ru, TeamViewer, Join.me	OTR, Tor, Smartphones, Zoho.com webmail, TrueCrypt	Tor+ Trilight Zone + Cspace + ZRTP VoIP client on Linux
Current Operational Target Use					
Current Low Priority/Previous Higher Priority Target Use					
Technical Thought Leader Recommendations, Experimentation					

TOP SECRET//COMINT//REL FVEY//20340601

Things become "catastrophic" for the NSA at level five - when, for example, a subject uses a combination of Tor, another anonymization service, the instant messaging system CSpace and a system for Internet telephony (voice over IP) called ZRTP. This type of combination results in a "near-total loss/lack of insight to target communications, presence," the NSA document states. (Der Spiegel)

Signal protocol

Open Whisper Systems developed cryptographic protocol Signal in 2013.

Currently the protocol is being implemented in:

- Facebook Messenger (July 2015) – monthly about a billion of users,
- WhatsApp (April 2016) – more than a billion of registered users,
- Google Allo (September 2016) – since October 2016 Google Allo is default messenger on Pixel mobile phones,
- Viber (May 2015) – partly implemented – it has more than 100 million of monthly active users.

Towards anonymity

Using of anonymisation network increases latency. So no real time communication is possible!

However, Signal supports voice messages, which can be sent over Tor network.

In group chat they can be used as fully anonymous push-to-talk system.

There are also being developed solutions which enable strong anonymity and solutions which does not need central infrastructure. Examples:

- **Ring** is VoIP client which supports decentralized communication, anonymous identities and peer-to-peer discovery and connection.
- **Briar** is peer-to-peer encrypted messaging and forums application, does not require internet access and does not use cloud.

Conclusion

Information security and encryption of communications is becoming widely adopted in last years.

Use of strong encryption is becoming simplified.

Average user does not need to be proactive to get security (and security updates) – security is becoming a norm.

Companies are paying attention to implementing security features, security testing, etc.

Legislation requires implementation of security practices.

Yes, there are still some problems, especially on a hardware level. But problems are being discussed and solutions sought.

Eavesdropping is becoming harder and more expensive.

Anonymity: how to reveal your real target???

Questions?

<https://pravokator.si>