


Phonebusters

Kako varni so v resnici
mobilni telefoni?

BUSTED!

Matej Kovačič

 Institut
"Jožef Stefan"
Ljubljana, Slovenija

OPOZORILO:
“kidz, don't try this at home”

Pri izvajanju varnostnih analiz je potrebno paziti na spoštovanje zakonodaje, izogibati se je potrebno povzročanju motenj na omrežju.

Prestrežanje tujih komunikacij je kaznivo.

Vdiranje v tuje sisteme in omrežja je kaznivo.

Oddajanje v nelicenciranem delu radijskega spektra je kaznivo.



Nevil Maskeyne (1863-1924)

Problem avtentikacije

Mobilna telefonija nima vgrajenih ustreznih mehanizmov overovitve.

Klicatelj oz. pošiljatelj SMS sporočila je "overjen" zgolj s svojo mobilno številko.

Rezultat: močno je ponarejanje klicne identitete!

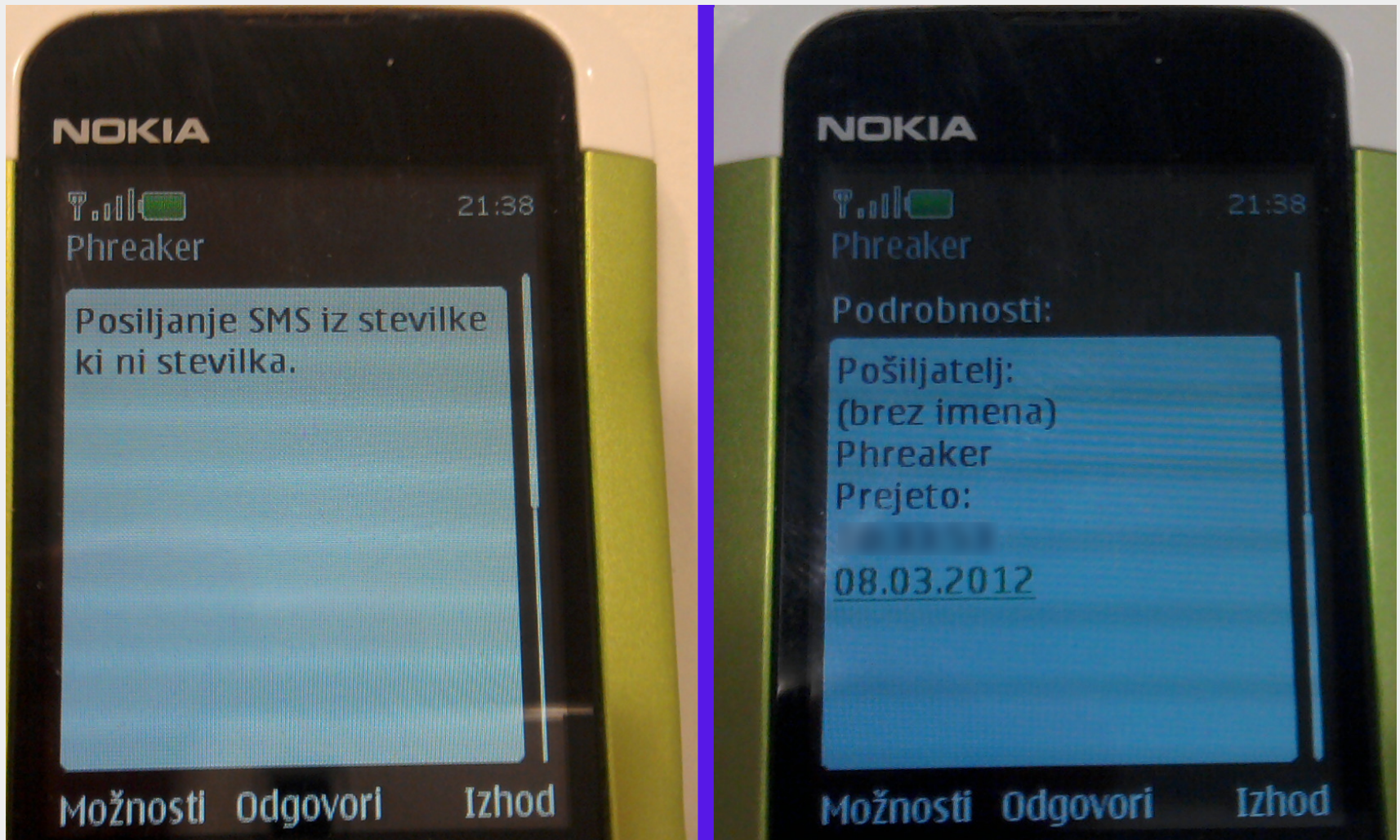
Overovitveni mehanizmi so pomanjkljivi tudi med operaterji.

Rezultat: mogoči so številni napadi na SS7 infrastrukturo!

Mobilno omrežje se ne avtenticira mobilnemu telefonu.

Rezultat: mogoče je uporabiti lažne bazne postaje (IMSI lovilce)!

Pošiljanje SMS sporočil z lažno identifikacijo



<[http://provider.com/sms/json?username=xxxxxxx&password=xxxxxxx&from=Phreaker&to=38631123456&text=Posiljanje e%20SMS%20iz%20številke%20ki%20ni%20številka.](http://provider.com/sms/json?username=xxxxxxx&password=xxxxxxx&from=Phreaker&to=38631123456&text=Posiljanje%20SMS%20iz%20številke%20ki%20ni%20številka.)>

Lažna klicna identifikacija

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	(Unspecified)
1000/1000	192.168.56.1

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

IAX2 Registry

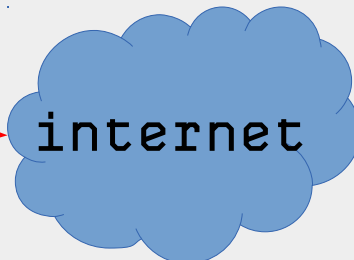
Host	dnsmgr	Username	Perceived	Refresh	State
0 IAX2 registrations.					

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 ~#
```



VPN

Lažna klicna identifikacija

The image shows two overlapping browser windows from Mozilla Firefox. The background window displays the 'PBX Status' page for 'trixbox1.localdomain'. The foreground window shows the 'Extension: 1000' configuration page. A red arrow points to the 'Display Name' field, which contains the text 'Matej 1'.

Background Window: PBX Status

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:

Name/username	Host
2000	(Unspecified)
1000/1000	192.168.56.1

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

IAX2 Registry: 0 IAX2 registrations.

IAX2 Peers:

Name/Username	Host	Ma
[Redacted]	(S)	25

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

Subscribe/Notif...

Foreground Window: Extension: 1000

System Status Packages PBX System Settings Help

Admin Reports Panel Recordings Help

English

Delete Extension 1000

Add Follow Me Settings

Add Extension

Matej 1 <1000>

Matej 2 <2000>

Edit Extension

Display Name: Matej 1

CID Num Alias: [Empty]

SIP Alias: [Empty]

Extension Options

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

Ring Time: Default

Call Waiting: Enable

Call Screening: Disable

Lažna klicna identifikacija



Lažna klicna identifikacija

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

Praktična "uporaba" :-)

GSM modul za odpiranje garažnih ali vhodnih vrat

Ponujamo vam uporabno napravo, ki z enostavnim telefonskim garažna ali vhodna vrata.

GSM modul je naprava, katero lahko avtorizirani uporabnik pokliče z avtomatizirana vrata. Naprava prepozna največ pet določenih telefonskih števil in se s takim klicem sproži odprtje ali zaprtje vrat.

IKU d.o.o. vam nudi:

- o dobavo paketa z navodili za uporabo,
- o montažo na dogovorjena mesta (pokličite nas in poslali vam bomo poštovsko).

Uporaba GSM modula za odpiranje vrat:

na avtomatizirana garažna, vhodna ali druga vrata se namesti GSM modul, ki preko GSM omrežja (mobilnih) števil, s katerimi je možno s hitrim telefonskim klicem omenjena vrata odpre ali zapre. Oziroma se lahko uporablja tudi za odpiranje vrat, kar pomeni, da odpade uporaba daljinskih upravljalnikov oziroma dodatnih naprav in aparatov, ker priložni telefon že »obvezna oprema« vseh ljudi.



voice

SMS



SMS PARKING



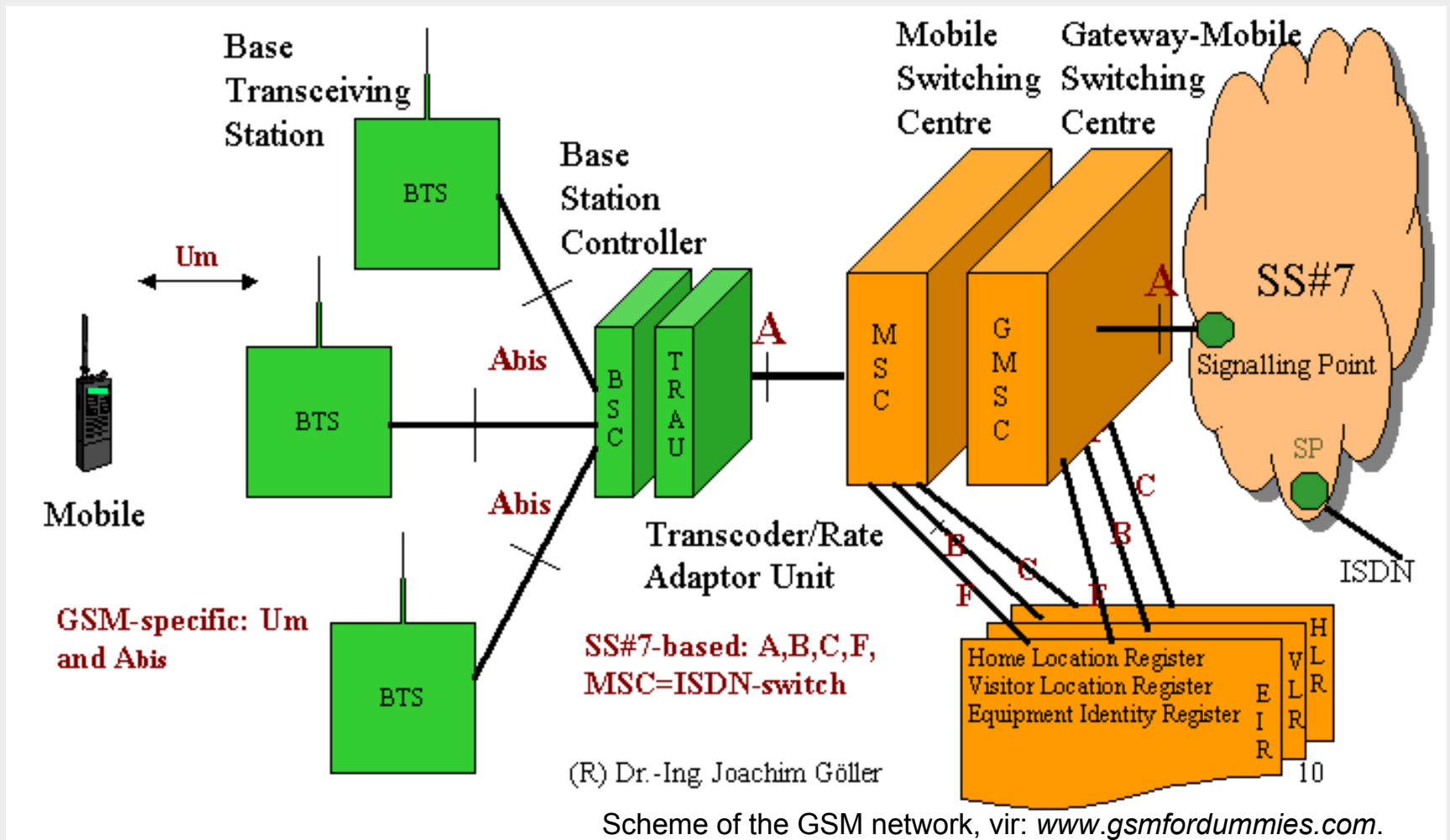
PLAČILO PARKIRNINE:

- 1 Na številko **041 20 20 10** pošljite SMS s cono, številko registrske tablice vozila in časom parkiranja s presledki za vozilo za katero želite plačati parkirnino.
Primer plačila parkirnine v coni B1 za 2 uri: **B1 LJ1234 2**
- 2 Prejeli boste brezplačno povratno SMS sporočilo, ki velja kot dokazilo o plačilu parkirnine. Plača se vsaka začeta ura.

REGISTRACIJA / POLNITEV RAČUNA:

Polnitev URBANA SMS Parking računa se lahko izvede na vseh Urbanomatih ali prodajnih mestih za polnitev in prodajo kartice Urbana (TIC, Kiosk DELO prodaja, Trafika 3 DVA, Pošta Slovenije, Petrol, Mercator, Spar, itd.). Registracija računa se izvede samodejno ob prvi polnitvi.

Nekaj osnov o GSM tehnologiji



SIM kartica in mobilna naprava, IMSI, TMSI, A5/x, "broadcast channels" in podatkovni kanali...

Zajemanje signala včasih...



1 Uporaba mobilnih telefonov s Calypso čipovjem...

```
matej@cryptopia: ~/osmocombb-raw/src/host/osmocon
Die ID code: 7e540b2fc90393bb
=====
REG_DPLL=0x2413
CNTL_ARM_CLK=0xf0a1
CNTL_CLK=0xff91
CNTL_RST=0xfff3
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 Povezava telefona in računalnika s posebnim kablom in nalaganje spremenjenega ROM-a...

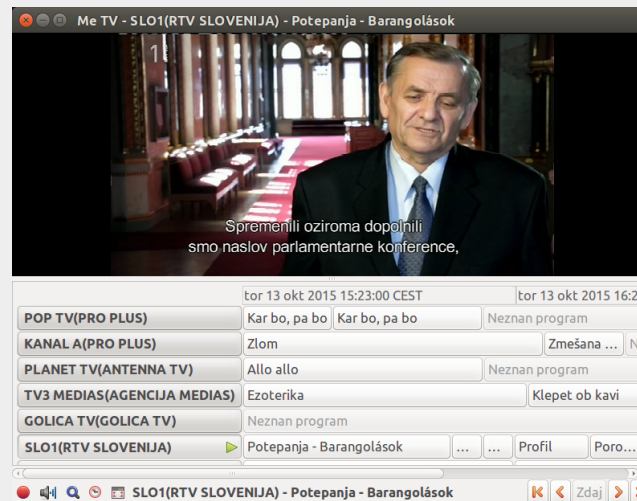
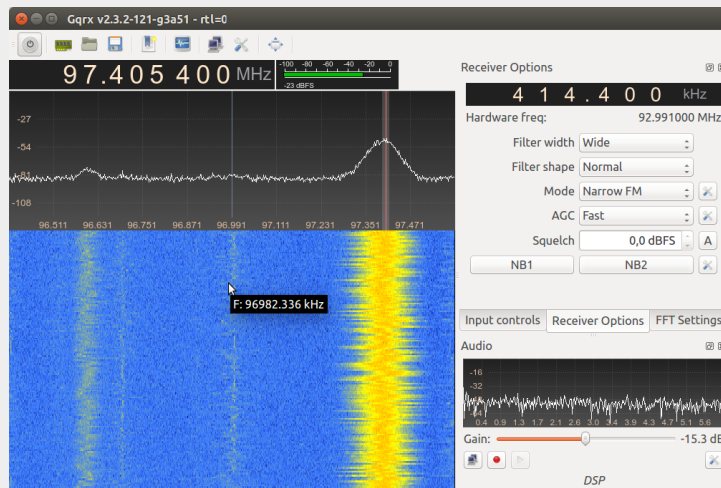
```
Failed to connect to '/tmp/osmocombb-raw/src/host/osmocon'.
Failed during sap.open(), no SIM reader
<000e> cell_log.c:803 Scanner initialized
Mobile initialized, please start phone now!
<000e> cell_log.c:367 Measure from 0 to 124
<000e> cell_log.c:367 Measure from 512 to 885
<000e> cell_log.c:367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

Zajemanje signala danes...



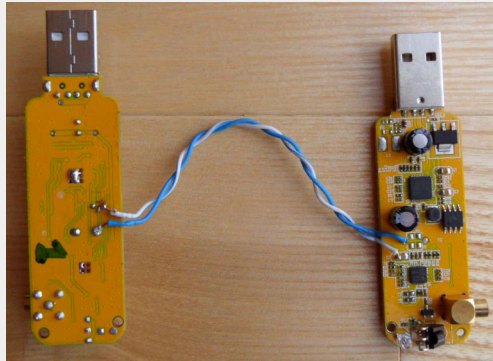
DVB-T naprava (z Elonics 4000 čipom; ~20 EUR).



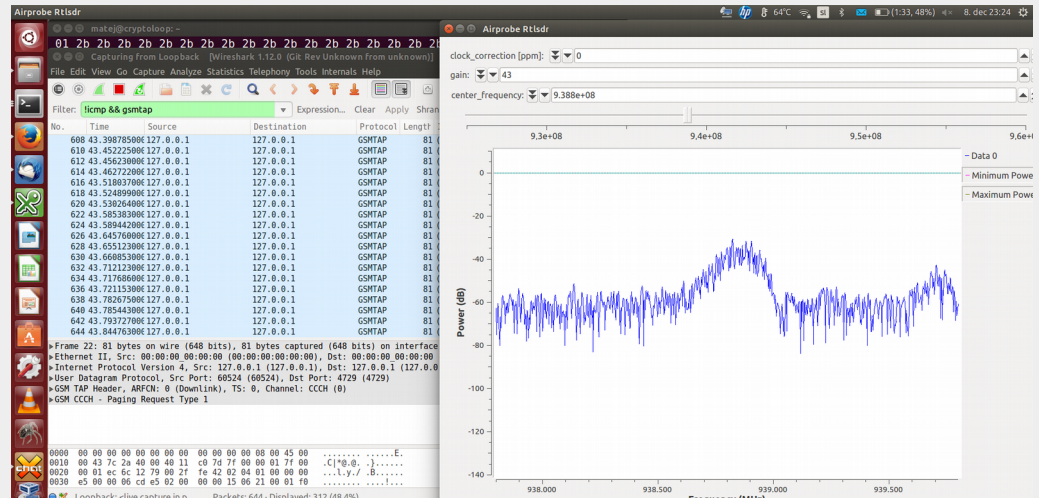
Orodje za zajem in analizo GSM signalov.

```
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
```

Varnostna analiza GSM v letu 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 ...
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: ...

Nekateri operaterji so uporabljali šifrirni algoritem A5/1...

Varnostna analiza GSM v letu 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
+

Če je mobilni telefon rekel, da podpira A5/3...

Varnostna analiza GSM v letu 2012

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

Filter: gsmtap

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

Frame 3934: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0

- Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
- User Datagram Protocol, Src Port: 45090 (45090), Dst Port: gsmtap (4729)
- GSM TAP Header, ARFCN: 101 (Downlink), TS: 1, Channel: SDCCH/8 (0)
- Link Access Procedure, Channel Dm (LAPDm)
- GSM A-I/F DTAP - Ciphering Mode Command
 - Protocol Discriminator: Radio Resources Management messages
 - DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
 - Cipher Mode Setting
 -1 = SC: Start ciphering (1)
 -000. = Algorithm identifier: Cipher with algorithm A5/1 (0)

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

...je omrežje odvrnilo, da podpira samo A5/1.

Varnostna analiza GSM v letu 2012

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

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

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

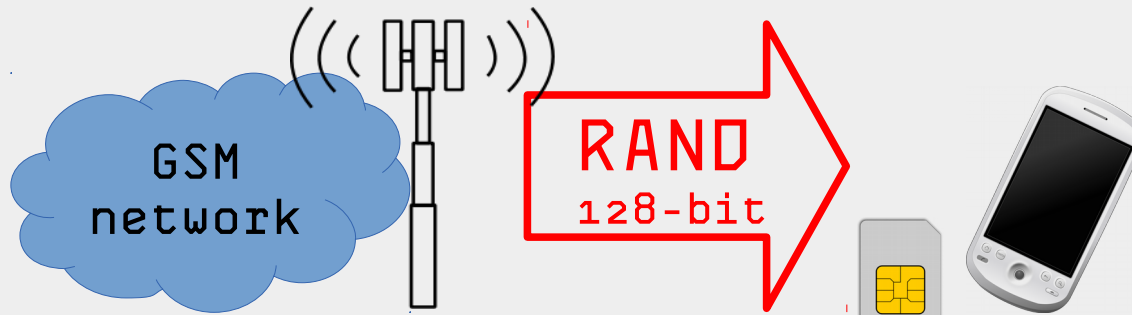
```
0010 00 43 4f b1 40 00 40 11 ec f6 7f 00 00 01 7f 00 .CO.@.@. ....
0020 00 01 e4 4c 12 79 00 2f fe 42 02 04 01 00 00 20 ...L.y./ .B....
0030 31 ff 00 19 7f 4b 08 00 05 00 03 00 0d 06 35 10 1....K.. .....5
0040 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b ++++++ ++++++
0050 2b +
```

V enem omrežju je bilo mogoče celo izključiti šifriranje...

GSM šifriranje

Šifrirni ključ ***Ki*** je shranjen na SIM kartici in v HLR registru. Sejni šifrirni ključ ***Kc*** se izračuna s pomočjo ***Ki*** in se uporablja za šifriranje SMS iz govorne komunikacije.

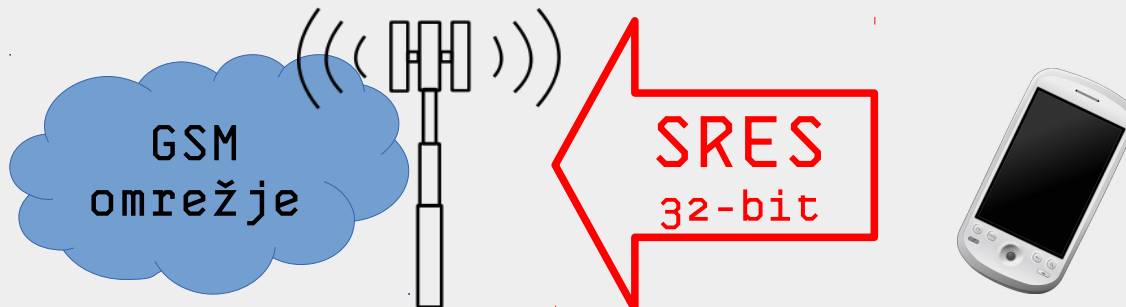
1.



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

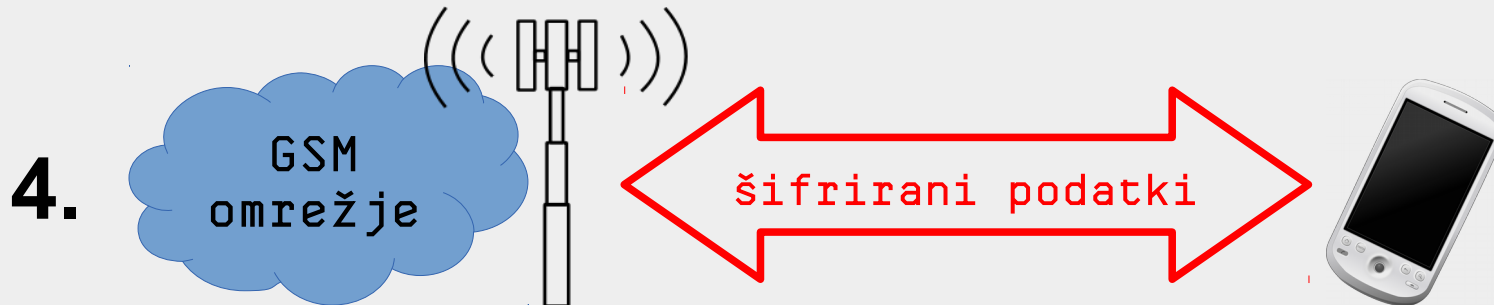
SIM kartica: $Ki + \text{RAND} @ A3 = \text{SRES}$

2.



GSM šifriranje

- 3.** Na obeh straneh se izračuna K_c (z uporabo algoritma A8):
 $K_i + \text{RAND} @ A8 = K_c$



Če je SRES na obeh straneh enak, imata omrežje in mobilni telefon enak K_c . To pomeni, da je sejni ključ »izmenjan« ne da bi bil prenesen čez omrežje. Zdaj se podatki šifrirajo z $K_c + A5/x$. »Po zraku« se prenašajo samo šifrirani podatki.

Kriptoanaliza GSM komunikacije

VSEBINA PODATKOVNEGA IZBRUHA V GSM

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

"ENKRATNI" KLJUČ ZA ŠIFRIRANJE PODATKOVNEGA TOKA

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

ŠIFRIRANO SPOROČILO (XOR)

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

$f(K_c)$



Kraken



K_c

Naključno vs. nenaključno bitno zapolnjevanje

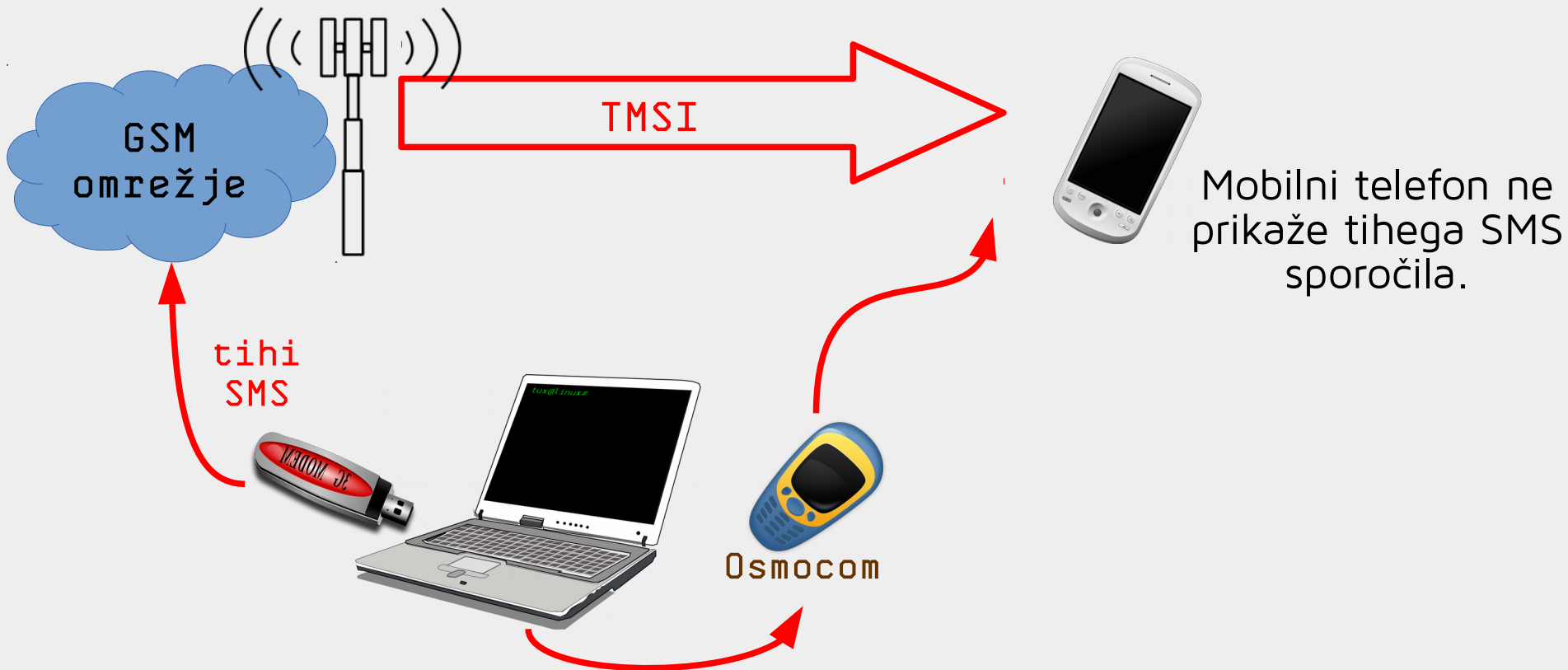
(*Random padding vs. non-random padding*)

```
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 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 08 .....y./ .B.....n
0030 bd 00 00 17 4c 9c 08 00 00 00 03 54 0d 05 18 03 ....L... ..T....
0040 92 da c9 32 8d 59 71 d1 8e ce 4e 6e 35 dd 65 25 ...2.Yq. ..Nn5.e%
0050 5d ]
```

Lociranje uporabnika v mobilnem omrežju

Na mobilno številko pričnemo pošiljati tihe SMS. Hkrati na omrežju opazujemo katera TMSI številka prejema (šifrirane) podatke.



Kriptoanaliza v praksi



- »Iz zraka« pasivno zajamemo šifrirane podatkovne pakete.
- Z ugibanjem vsebine GSM izbruha (ugibanjem zapolnitvenih bitov) izračunamo »enkratni« šifrirni ključ.
- S pomočjo kriptoanalize rekonstruiramo sejni ključ K_c .
- V procesu ne potrebujemo fizičnega dostopa ne do SIM kartice, ne do mobilnega telefona niti do mobilnega omrežja!



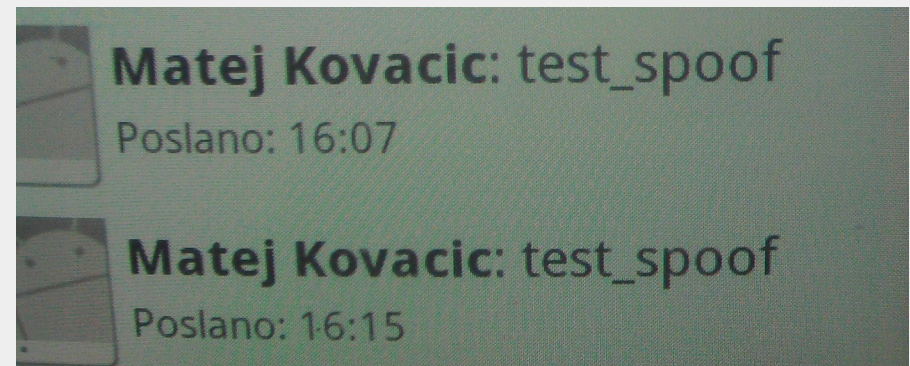
Ponarejanje mobilne *identitete*

Za ponarejanje mobilne **identitete** potrebujemo:

- IMSI številka (jo pridobimo z SS7 vpogledom),
- TMSI številka (jo zajamemo iz omrežja),
- sejni šifrirni ključ (ga pridobimo s kriptanalizo),
- zaporedna številka ključa (ang. *key sequence number* – jo zajamemo iz omrežja).

Če omrežje uporablja A5/0, potrebujemo samo TMSI in zaporedno številko ključa – kriptanaliza ni potrebna!

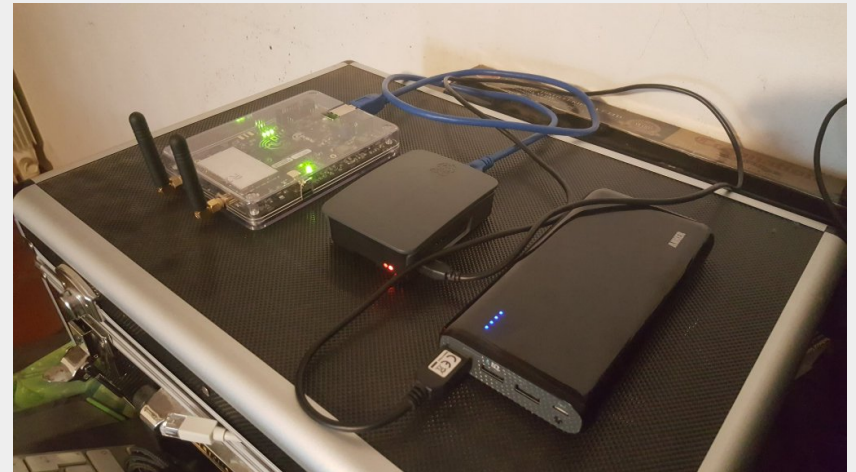
```
matej@cryptopia: ~
matej@cryptopia: ~
testcard      Attach built in test SIM
spooft        Attach spoofing SIM
reader        Attach SIM from reader
remove        Detach SIM card
pin           Enter PIN for SIM card
disable-pin   Disable PIN of SIM card
enable-pin    Enable PIN of SIM card
change-pin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



Dve SMS sporočili poslani z lažno mobilno identiteto.

Lovilci IMSI številk

V osnovi so to lažne bazne postaje.



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 lovilci – kako delujejo?

Najprej se lažno predstavijo kot legitimna bazna postaja nekega omrežja.

Nato mobilnim telefonom v bližini sporočijo lažno LAC kodo (*Location Area Code*).

Zdaj mobilni telefoni kontaktirajo IMSI lovilec (z tim. *Location Update* proceduro), a s svojo TMSI številko.

IMSI lovilec se zdaj zlaže, da je TMSI številka potekla in zahteva ponovno avtentikacijo (tim. *re-authentication*).

Mobilni telefoni zdaj lovilcu javijo svoji IMSI in IMEI številki.

IMSI lovilec zdaj reče, da ne more sprejeti telefona (*Location Update Reject*) in ga preusmeri nazaj k izvornemu omrežju.

Ali pa tudi ne... v tem primeru lovilci s telefonom lahko počnejo še marsikaj...

IMSI lovilci - jih lahko zaznamo?

Wireshark interface showing network traffic analysis. The packet list pane displays two packets (No. 24 and 34) of type GSM TAP, both with source and destination IP 127.0.0.1 and protocol GSMTAP. The packet details pane shows the structure of the GSM TAP header, including the GSM CCCH - Paging Request Type 1 section. The IMSI field is highlighted in orange and contains a redacted value. The packet bytes pane shows the raw hex and ASCII data for the IMSI field.

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

▶ 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

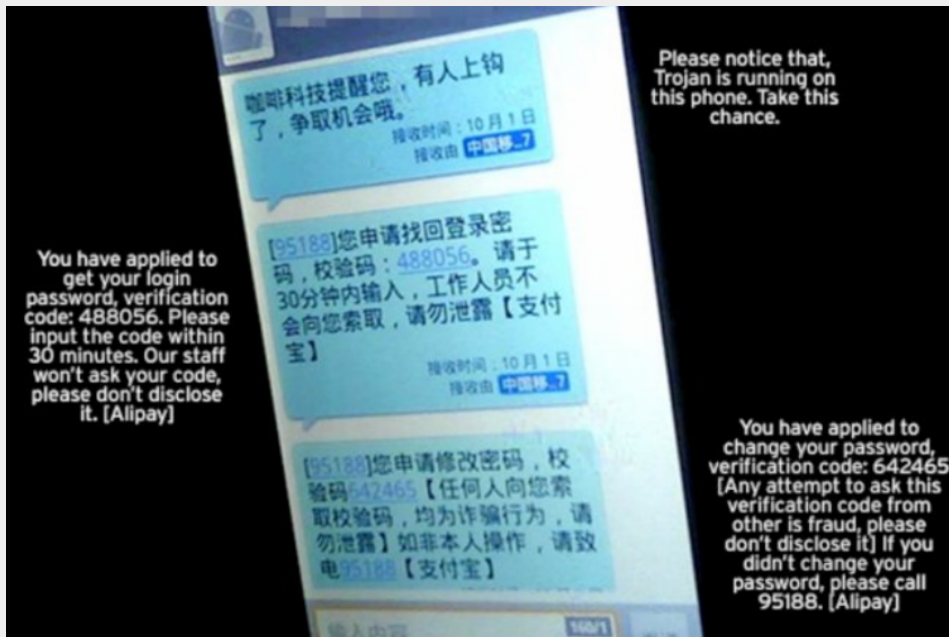
```
0010 00 43 70 31 40 00 40 11 cc 76 7f 00 00 01 7f 00 .Cp1@.@. .v.....
0020 [REDACTED] [REDACTED]
0030 [REDACTED] [REDACTED]
0040 [REDACTED] 2b 2b [REDACTED] +++++
0050 2b +
```

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

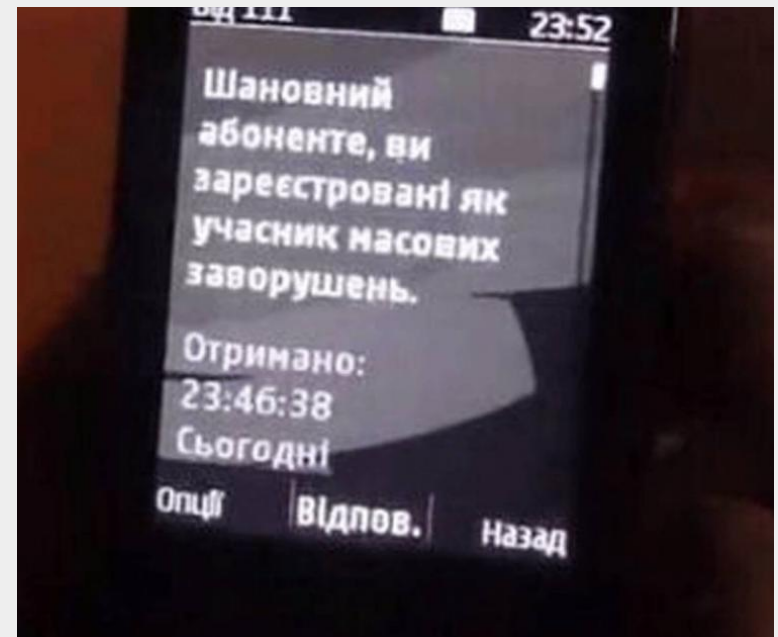
IMSI lovilci – kaj zmorejo?

IMSI lovilci lahko:

- **razkrijejo lokacijo** mobilnega telefona,
- mobilnemu telefonu ponudijo omrežno povezljivost in izvedejo **napad s posrednikom** (tim. **MITM napad**),
- pokličejo telefon ali mu pošljejo SMS **mimo omrežja**.



Kitajska SMS SPAM sporočila.

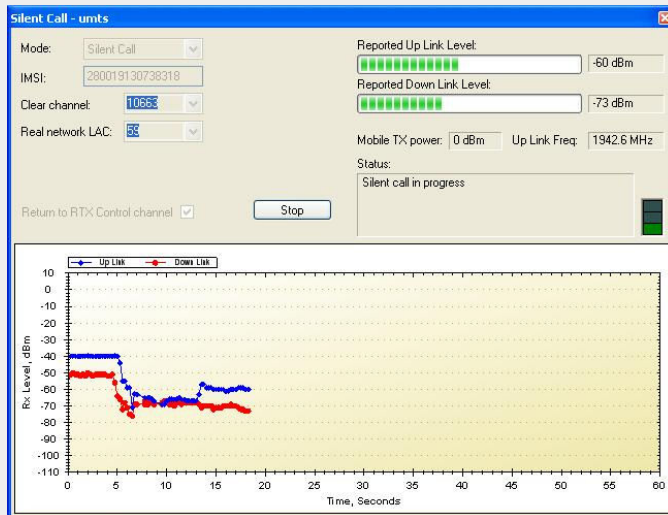


Ukrajina – sporočilo protestnikom.

IMSI lovilci - kaj zmorejo?

IMSI lovilci lahko tudi:

- **izolirajo** mobilni telefon od omrežja,
- mobilni telefon **začasno onemogočijo** (tako, da je potreben ponovni zagon) ali mu hitro **izpraznijo baterijo**,
- izvedejo **tihi klic**, kar omogoča prisluškovanje okolici telefona,
- na daljavo **namestijo zlonamerno programsko opremo** (tim. *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

Nekateri SS7 napadi

Signalling System #7 je protokol za izmenjavo podatkov med telefonskimi operaterji.

SS7 omogoča dostop do Home Location Registra, Visitor Location Registra in Mobile Switching Centra...

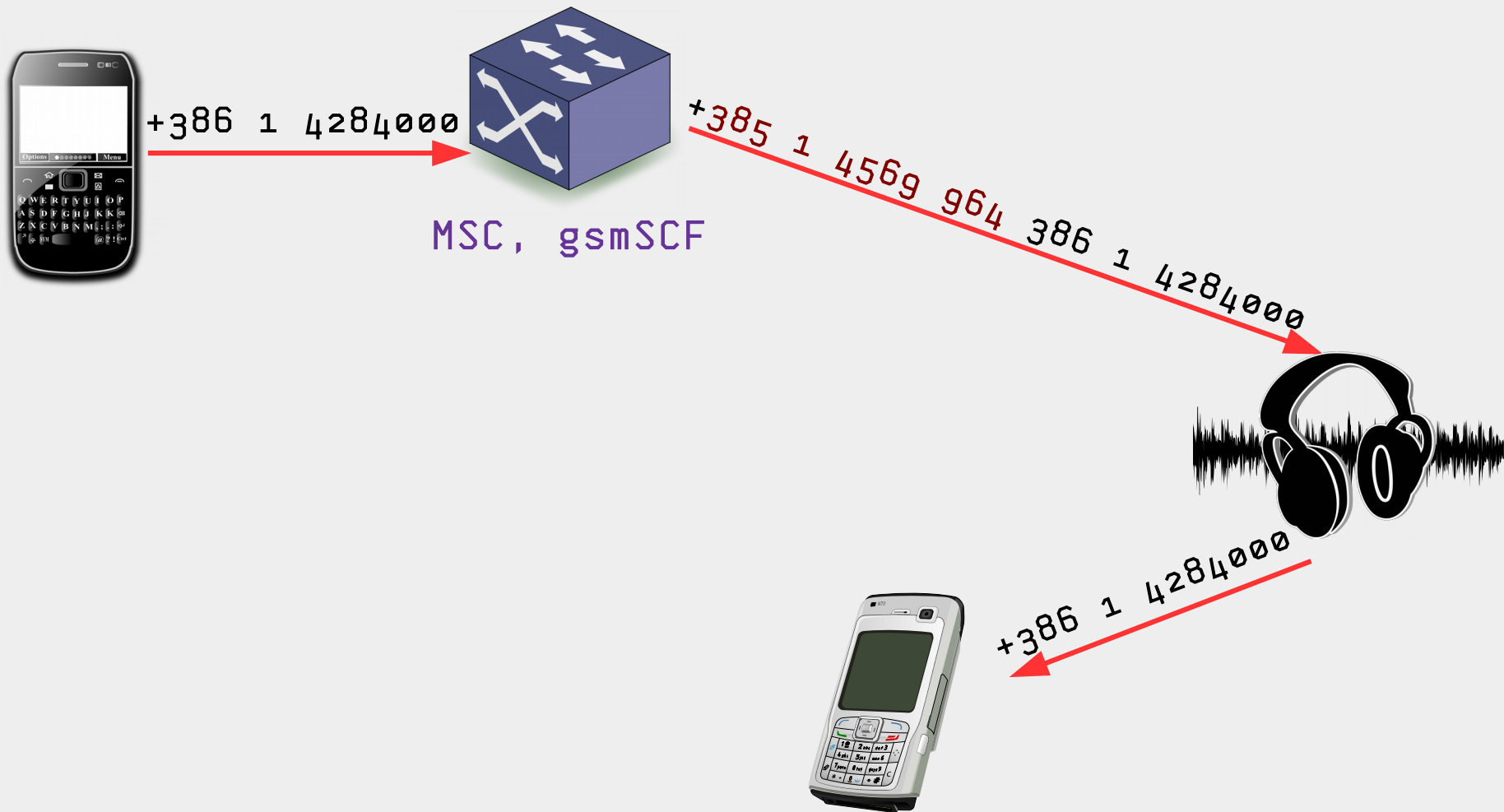
Vendar pa je avtentikacija v SS7 pomanjkljiva. Zato je z zlorabo SS7 mogočih nekaj zanimivih napadov...

Legitimna uporaba: CAMEL (*Customised Applications for Mobile networks Enhanced Logic*):

- Uporabnik gostuje v tujem omrežju.
- Uporabnikov HLR pove gostujočemu VLR, naj MSC pred vsakim klicem, ki ga želi opraviti uporabnik, kontaktira gsmSCF (*GSM Service Control Function*) v domačem omrežju in vpraša kaj naj stori s klicem.
- Če uporabnik kliče "lokalno številko", gsmSCF številko prepíše v mednarodni format (+386...) in sporoči MSCju naj pokliče to številko.

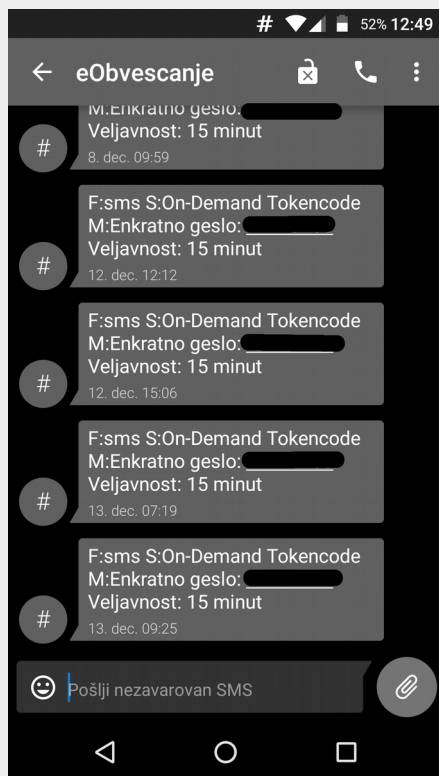
Primer: preusmerjanje odhodnih klicev

gsmSCF funkcijo pa je mogoče tudi zlorabiti...



Primer: preusmerjanje dohodnih klicev

Napadalec se pretvarja, da uporabnik gostuje v njegovem omrežju... Od te točke dalje so vsi dohodni klici in SMS sporočila preusmerjeni k napadalcu.



Zdaj se žrtev želi prijaviti v bančni račun. Ker uporablja dvofaktorsko avtentikacijo, ji banka pošlje SMS sporočilo z mTAN dostopno kodo...

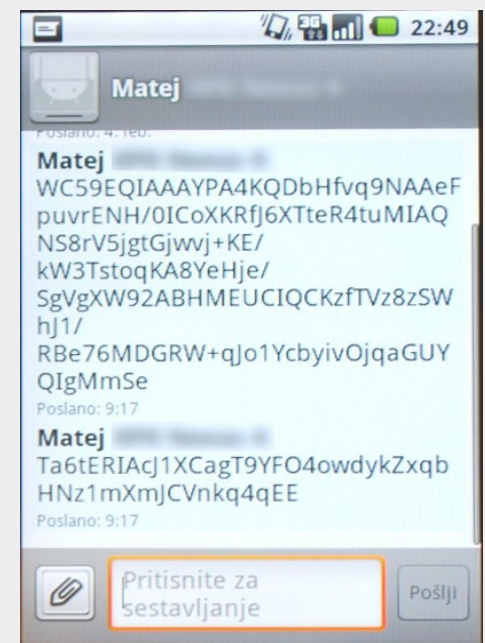
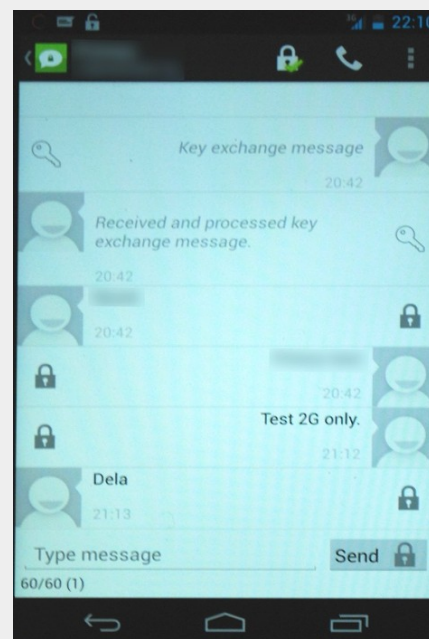
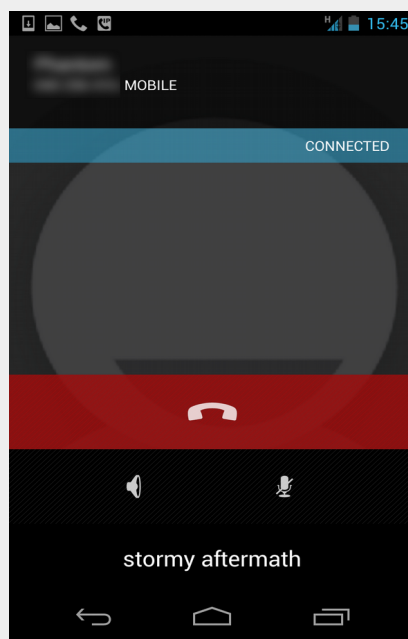
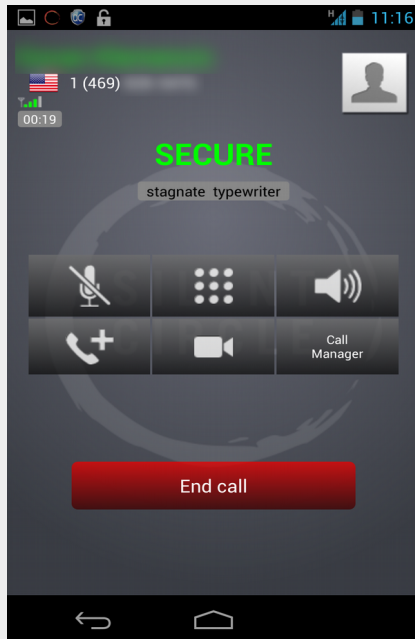
Ali pa se žrtev želi prijaviti v interno omrežje slovenske vlade... :-)

BUSTED!

Zaščita



Šifriranje mobilnih komunikacij



Rešitev: uporaba podatkovnega prenosa in šifriranje komunikacij na nivoju aplikacij.

Nešifriran in šifriran telefonski klic

The image displays a network analysis setup for a VoIP call. The main window is Wireshark, showing a capture of SIP messages. A red box highlights the INVITE and ACK messages, indicating the start and end of the call setup. Below this, the RTP Player window shows the audio stream being played back. The RTP Player window includes a waveform visualization and a frequency spectrum plot. The frequency spectrum plot shows a peak at 44100 Hz, indicating the audio sample rate. The RTP Player window also displays the audio format as Mono, 44100Hz, 32-bitno plavajoče.

Wireshark Filter: Expression... Clear Apply Shrni

No.	Time	Source	Destination	Length	Protocol	Info
1	20:10:32.318	[redacted]	[redacted]		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	[redacted]	<sip:031[redacted]	SIP 7 COMPLETE
7	20:10:39.671	102,384695	160,364970	172.16.0.116	"Matej Kovaric" <sip:[redacted]	SIP 14 COMPLETE
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					

Detected 2 VoIP Calls. Selected 1 Call.

Start Time	Stop Time	Initial Speaker	From	To	Protoco	Packets	State	Comments
21,162982	88,346119	[redacted]	<sip:031[redacted]	[redacted]	SIP	7	COMPLETE	
102,384695	160,364970	172.16.0.116	"Matej Kovaric" <sip:[redacted]	[redacted]	SIP	14	COMPLETE	

encrypted_srtp_audio

44100 Hz

32-bitno plavajoče

Utisaj Solo

44100 Hz

32-bitno plavajoče

Utisaj Solo

44100 Hz

32-bitno plavajoče

Utisaj Solo

44100 Hz

32-bitno plavajoče

Utisaj Solo

Aplikacija Signal

Za šifriranje mobilnih komunikacij obstaja več aplikacij.

Ena izmed boljših je aplikacija Signal, podjetja Open Whisper Systems. Na tehnični ravni uporablja:

- močne šifrirne algoritme,
- poudarjeno zaupnost (*perfect forward secrecy* ter *future secrecy*),
- zaznavanje napadov s posrednikom (MITM napadov),
- šifriranje od začetne do končne točke (tim. »end-to-end« šifriranje),
- podporo asinhroni komunikaciji,
- šifrirno lokalno shrambo sporočil.

Tehnična rešitev **preprečuje** prisluškovanje na omrežju ter s strani operaterja.

Aplikacija Signal

Uporabniški vidik:

- enostavna za uporabo,
- brezplačna,
- odprtokodna,
- aplikacija je bila varnostno preverjena.



“ 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 screenshot of the Signal website homepage. At the top, it says "A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION" with search, language, and menu options. The main heading is "SURVEILLANCE SELF-DEFENSE" with a graphic of two figures holding a shield. Below that, it says "Tips, Tools and How-tos for Safer Online Communications". A large red banner at the bottom asks "Want a security starter pack?" and says "Start from the beginning with a selection of simple steps."



“ 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



“ 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

Aplikacija Signal

Na strežnikih se beleži minimalno število prometnih podatkov.

Attachment A

<u>Account</u>	<u>Information</u>
██████████	N/A
██████████	Last connection date: ██████████ Unix millis Account created: ██████████ Unix millis

Mogoča je dodatna anonimizacija:

- uporaba OWS posredniškega strežnika,
- registracija "nepovezane telefonske številke",
- teoretično: uporaba preko Tor omrežja,
- aplikacija vsebuje tudi tehnologije za zaobid cenzure (tim. *domain fronting*).

Tehnologijo »priporočča« celo NSA! :-)

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 protokol

Pri Open Whisper Systems so v letu 2013 razvili kriptografski protokol Signal.

Trenutno je protokol implementiran v:

- *Facebook Messenger* (od julija 2015) – mesečno ima okrog milijardo uporabnikov,
- *WhatsApp* (od aprila 2016) – ima več kot milijardo registriranih uporabnikov,
- *Google Alo* (od septembra 2016) – od oktobra 2016 je Google Alo privzeta aplikacija za sporočila na Pixel mobilnih telefonih,
- *Viber* (od maja 2015) – implementiran samo delno – ima več kot 100 milijonov mesečno aktivnih uporabnikov.

Vseeno pa je aplikacija Signal še zdaleč najbolj varna rešitev.

Anonimnost mobilnih komunikacij

Uporaba anonimizacijskih tehnologij povečuje latenco. Zato realnočasovna (govorna) komunikacija ni mogoča!

Vendar pa Signal podpira pošiljanje zvočnih sporočil. Pošiljati jih je mogoče preko omrežja Tor.

V skupinskih pogovorih jih je mogoče uporabiti kot popolnoma anonimnen PTT ("push-to-talk") sistem.

Nekateri razvijajo tudi rešitve, ki omogočajo visoko anonimnost in celo ne potrebujejo centralne infrastrukture. Primeri:

- **Ring** je VoIP odjemalec, ki podpira decentralizirano komunikacijo, anonimne identitete P2P iskanje in P2P povezave.
- **Briar** (še v razvoju) je aplikacija za pošiljanje šifriranih sporočil in izmenjavo preko forumov, uporablja P2P povezovanje, ne potrebuje internetne povezave (!) in ne uporablja oblačnih rešitev.

Zaključek

Šifriranje komunikacij postaja v zadnjih letih čedalje bolj razširjeno.

Uporaba močnega šifriranja je postala enostavna.

Povprečnemu uporabniku je treba biti čedalje manj proaktiven glede varnosti – varnostne posodobitve se nameščajo samodejno, rešitve imajo že vgrajene varnostne mehanizme,.....

Podjetja čedalje več pozornosti namenjajo implementaciji varnostnih rešitev, varnostnemu testiranju, itd..

Tudi zakonodaja zahteva implementacijo varnostnih rešitev.

Težave še vedno ostajajo, zlastni na nivoju strojne opreme in strojne programske opreme, a se stanje izboljšuje.

Prisluškovanje postaja čedalje težje in čedalje dražje.

Anonimnost: kako sploh odkriti pravo tarčo???



Vprašanja?

Matej Kovačič
matej.kovacic@ijs.si

<https://pravokator.si>