

Varnost mobilne telefonije in zanesljivost prometnih podatkov

ter posledice tehnološkega razvoja za kazensko pravo



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

Fakulteta za logistiko | Celje, december 2013

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

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

Varnost skozi transparentnost

- **Kerchoffsov zakon** pravi, da je dober šifrirni sistem varen, tudi če je o njem znano vse, razen šifrirnega ključa.
 - Zavrača načelo, da je mogoče varnost zagotoviti s skrivanjem (t. i. *'security through obscurity'*).
 - Ne zahteva, da je šifrirni sistem javen, temveč le opozarja na to, da skrivnost ne zagotavlja varnosti, marveč jo v resnici lahko celo ogroža.
- Claude Shannon je postavil tim. Shannonovo maksimo, ki pravi, da sovražnik pozna šifrirni sistem.
- Eric S. Raymond pravi: *“Vsaka varnostna programska oprema, ki ne predpostavlja, da sovražnik poseduje izvorno kodo, je nevredna zaupanja; zatoorej: nikoli ne zaupaj zaprti kodi.”*

Varnost skozi transparentnost

- Korist od javne objave šifrirnih algoritmov je predvsem v tem, da lahko drugi kriptologi algoritem ali zamisel ocenijo in kritično ovrednotijo.
- To pripomore k izboljšavi kakovosti in k hitrejšemu razvoju.
- Pri zaprtih sistemih je veliko večja verjetnost, da je v njih kakšna napaka, ki bi jo javni pregled verjetno odkril, avtorji pa bi s tem dobili možnost, da jo odpravijo.

Varnost skozi transparentnost

- *Ne spominjam se nobenega kriptografskega sistema, razvitega na skrivaj, v katerem ne bi, potem ko je bil razkrit javnosti, kriptografska skupnost našla napake.*
--Bruce Schneier
- *But there's an old saying inside the NSA: "Attacks always get better; they never get worse."*
--Bruce Schneier

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

Pri izvajanju opisanih postopkov smo uporabili atestirano opremo oz. izvajali analizo lastnih komunikacij, prav tako v slovenskih GSM omrežjih nismo povzročali kakršnihkoli motenj.

Pri izvajanju varnostnega pregleda nismo klonirali SIM kartice niti pridobili ali rekonstruirali Ki ključa.

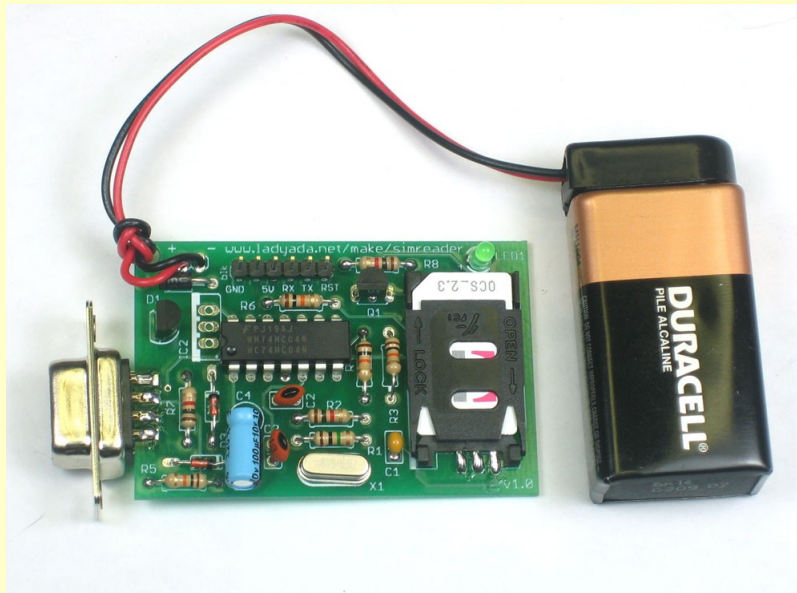
Namen raziskave je bil opozoriti na varnostne ranljivosti v slovenskih GSM omrežjih z željo, da se varnostne ranljivosti odpravijo, posledično pa se poveča stopnja varnosti in zasebnosti uporabnikov mobilne telefonije, ter z željo, da slovenski operaterji mobilne telefonije začnejo več vlagati v varnost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

Prav tako smo z raziskavo pokazali na pomanjkljivosti pri sistemu hrambe prometnih podatkov (tim. data retention) oziroma dokazno vrednost prometnih podatkov v kazenskem postopku postavili pod vprašaj.

Verodostojnost digitalnih podatkov na SIM kartici

Podatki iz SIM kartice

1: čitalec SIM kartic



Podatki iz SIM kartice

2: spreminjanje vsebine in metapodatkov SMS sporočil na SIM kartici

SMS edit

Message Text (44 / 160)

Septembra 2001 bo teroristicni napad na W TC.

Date: Fri Jan 12 1
From: 640 [REDACTED]
Status: Deleted

Save Prekliči

(2/35) sms messages

| Status | Date | From | Message |
|--------|--------------------------|-------------------|--|
| Read | Wed Oct 15 16:04:57 2014 | 123456 | Sporocilo iz prihodnosti... |
| Read | Fri Jan 12 18:54:37 2001 | +38640 [REDACTED] | Septembra 2001 bo teroristicni napad na WTC. |

SMS_export.txt (~/.Namizje/SIMreader) - gedit

```
# Date, From, ServiceCenter, Message
Wed Oct 15 16:04:57 2014,123456,+38641001333,Sporocilo iz prihodnosti...
Fri Jan 12 18:54:37 2001,+38640 [REDACTED],+38641001333,Septembra 2001 bo teroristicni napad na WTC.
```

Običajno besedilo | Širina tabulatorja: 8 | Vr. 2, St. 70 | VST

SIM Information

Location: 293F40
MSISDN: 000000486
Serial number: 89386400707
IMSI number: 2934001135
SIM phase: Phase 2+

| | Activated | Tries left |
|------|-----------|------------|
| PIN1 | Yes | 3 |
| PIN2 | Yes | 3 |

Podatki iz SIM kartice

3: rezultat



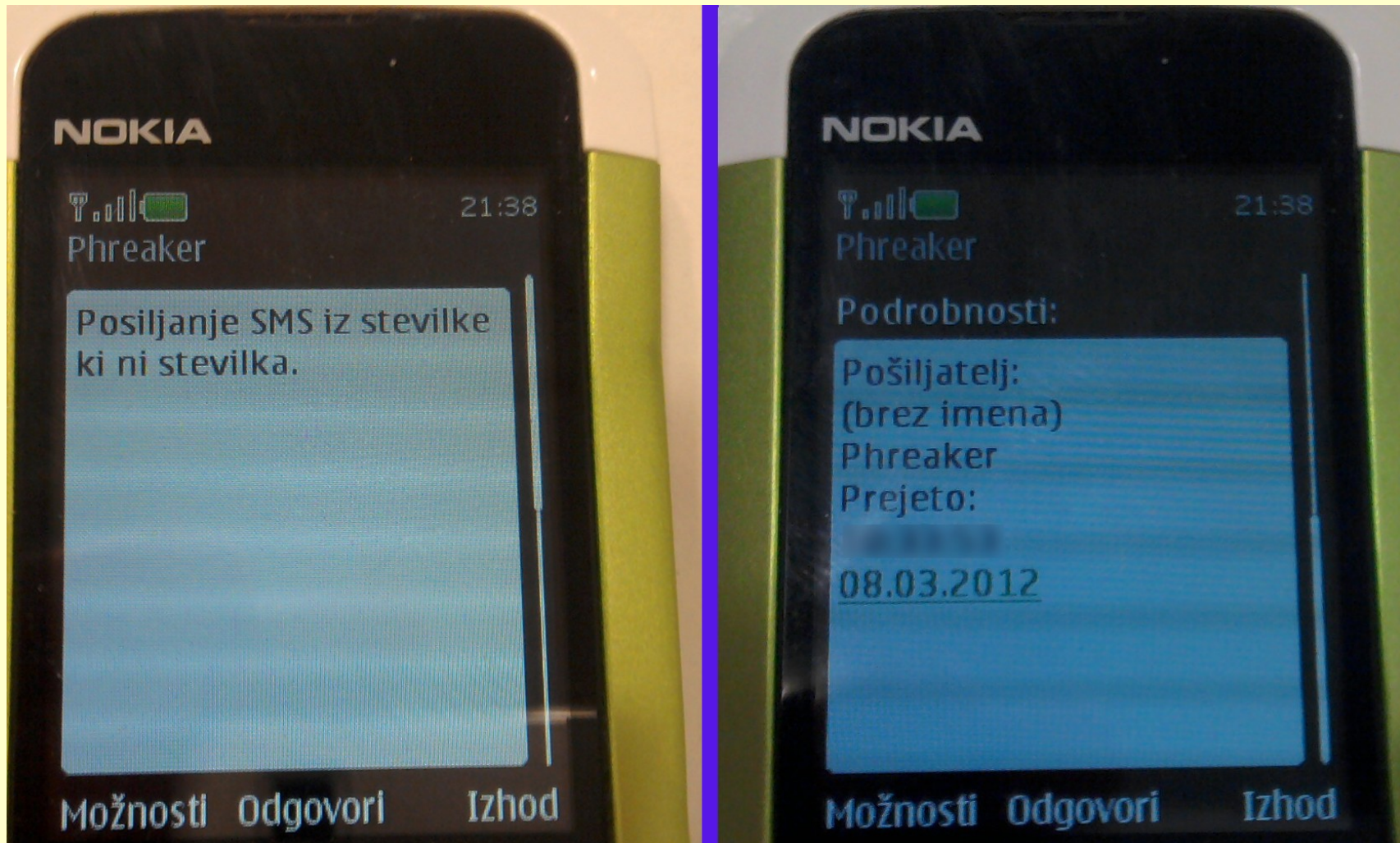
Pošiljanje SMS sporočil s spremenjeno klicno identifikacijo

Pošiljanje SMS sporočil "iz" poljubne številke

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



Pošiljanje SMS sporočil "iz" poljubne številke

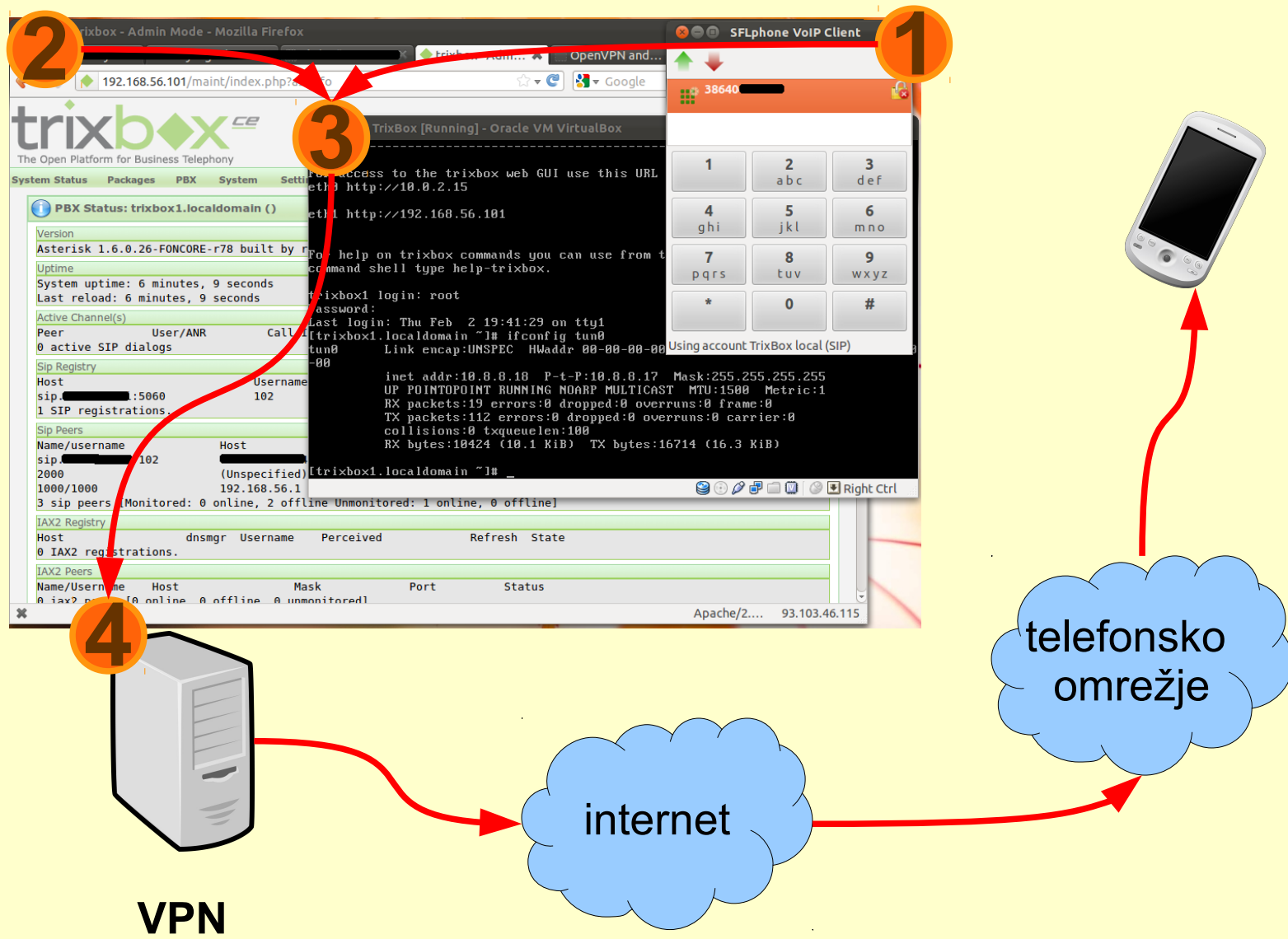


Klicanje s poljubno klicno identifikacijo

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

Klicanje s poljubno klicno identifikacijo

1: vzpostavitev infrastrukture



Klicanje s poljubno klicno identifikacijo

2: pogled v virtualno telefonsko centralo

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

Background Window: PBX Status

Version: Asterisk 1.6.0.26-FONCORE-r78 built by root @ revision 10000

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 | Dyn | Nat | Auth |
|---------------|---------------|-----|-----|------|
| 2000 | (Unspecified) | D | N | A |
| 1000/1000 | 192.168.56.1 | D | N | A |

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

IAX2 Registry: 0 IAX2 registrations.

IAX2 Peers:

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

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

Foreground Window: Extension: 1000

Display Name: Matej 1

CID Num Alias: [REDACTED]

SIP Alias: [REDACTED]

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

Ring Time: Default

Call Waiting: Enable

Call Screening: Disable

A red arrow points to the Outbound CID field.

Klicanje s poljubno klicno identifikacijom

3: rezultat na telefonu



Klicanje s poljubno klicno identifikacijo

4: prometni podatki pri operaterju

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

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

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

Praktične posledice :-)

GSM modul za odpiranje garažnih ali vhodnih vrat

Ponujamo vam uporabno napravo, ki z enostavnim telefonskim klicem odpre ali zapre avtomatizirana garažna ali vhodna vrata.

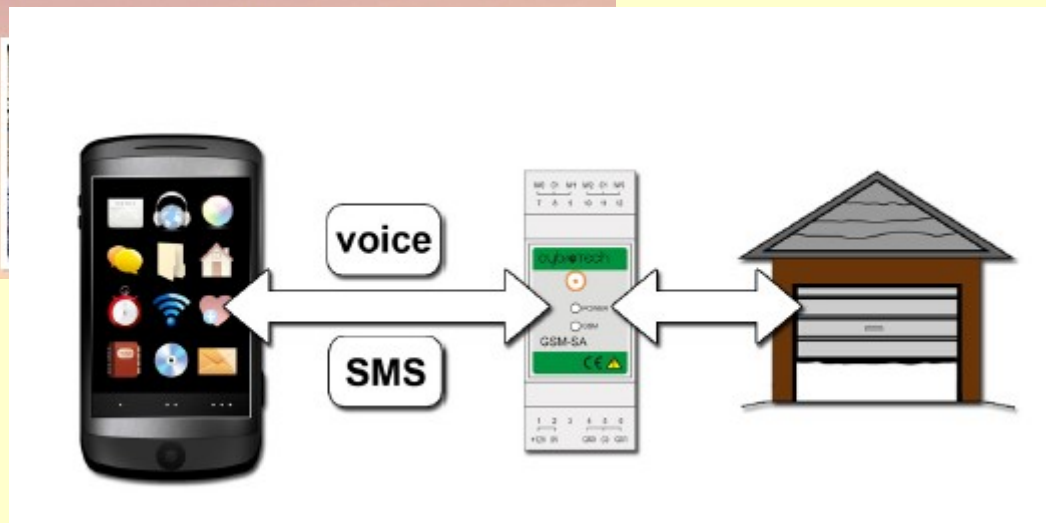
GSM modul je naprava, katero lahko avtorizirani uporabnik pokliče z namenom, da s hitrim klicem odpre ali zapre avtomatizirana vrata. Naprava prepozna največ pet določenih telefonskih števil, iz katerih se lahko na GSM modul pokliče in se s takim klicem sproži odprtje ali zaprtje vrat.

IKU d.o.o. vam nudi:

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

Uporaba GSM modula za odpiranje vrat:

na avtomatizirana garažna, vhodna ali druga vrata se namesti GSM modul, v katerega se zapiše do pet telefonskih (mobilnih) števil, s katerimi je možno s hitrim telefonskim klicem omenjena vrata odpreti ali zapreti. S tem načinom odpade uporaba daljinskih upravljalnikov oziroma dodatnih naprav in aparatov, ker predpostavljamo, da je mobilni telefon že »obvezna oprema« vseh ljudi.



Varnost slovenskih GSM omrežij

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).

Decoding GSM. 2010. Magnus Glendrange, Kristian Hove in Espen Hvideberg, Norwegian University of Science and Technology, Department of Telematics.

<<http://ntnu.diva-portal.org/smash/get/diva2:355716/FULLTEXT01>>

Kaj točno smo naredili?

(in zakaj to ni nezakonito)

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

Kaj točno smo naredili?

(in zakaj to ni nezakonito)

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

Kaj točno smo naredili?

(in zakaj to ni nezakonito)

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

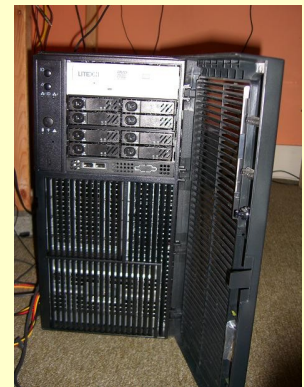
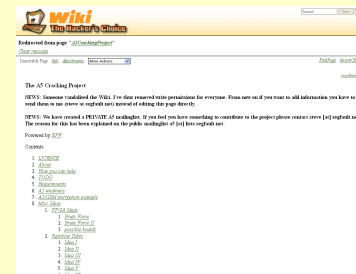
Predzgodba



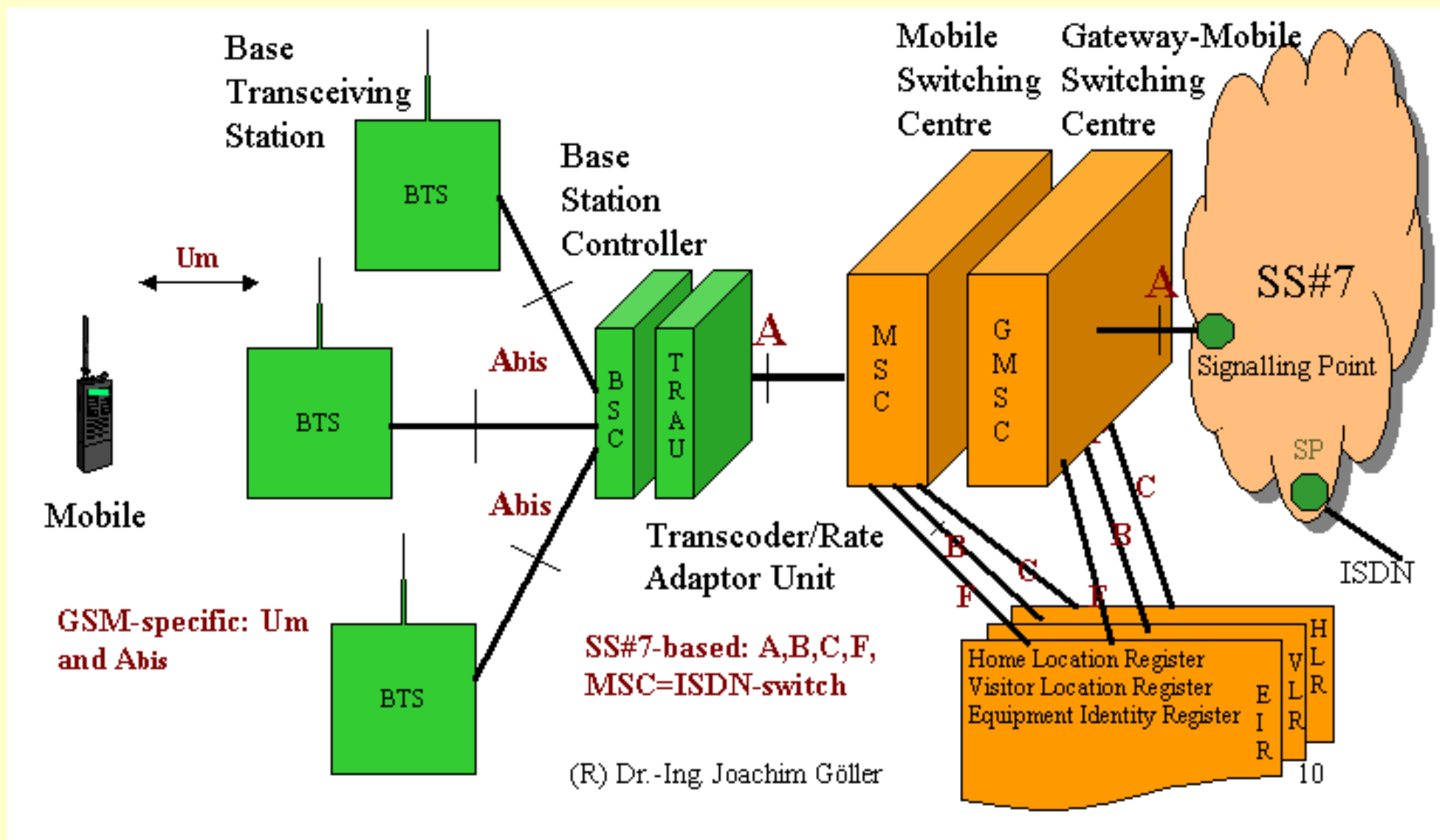
John Nevil Maskelyne
(1839 – 1917)



Kiberpipa
(2012)



Nekaj osnov o GSM



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

Shema GSM omrežja, vir: www.gsmfordummies.com.

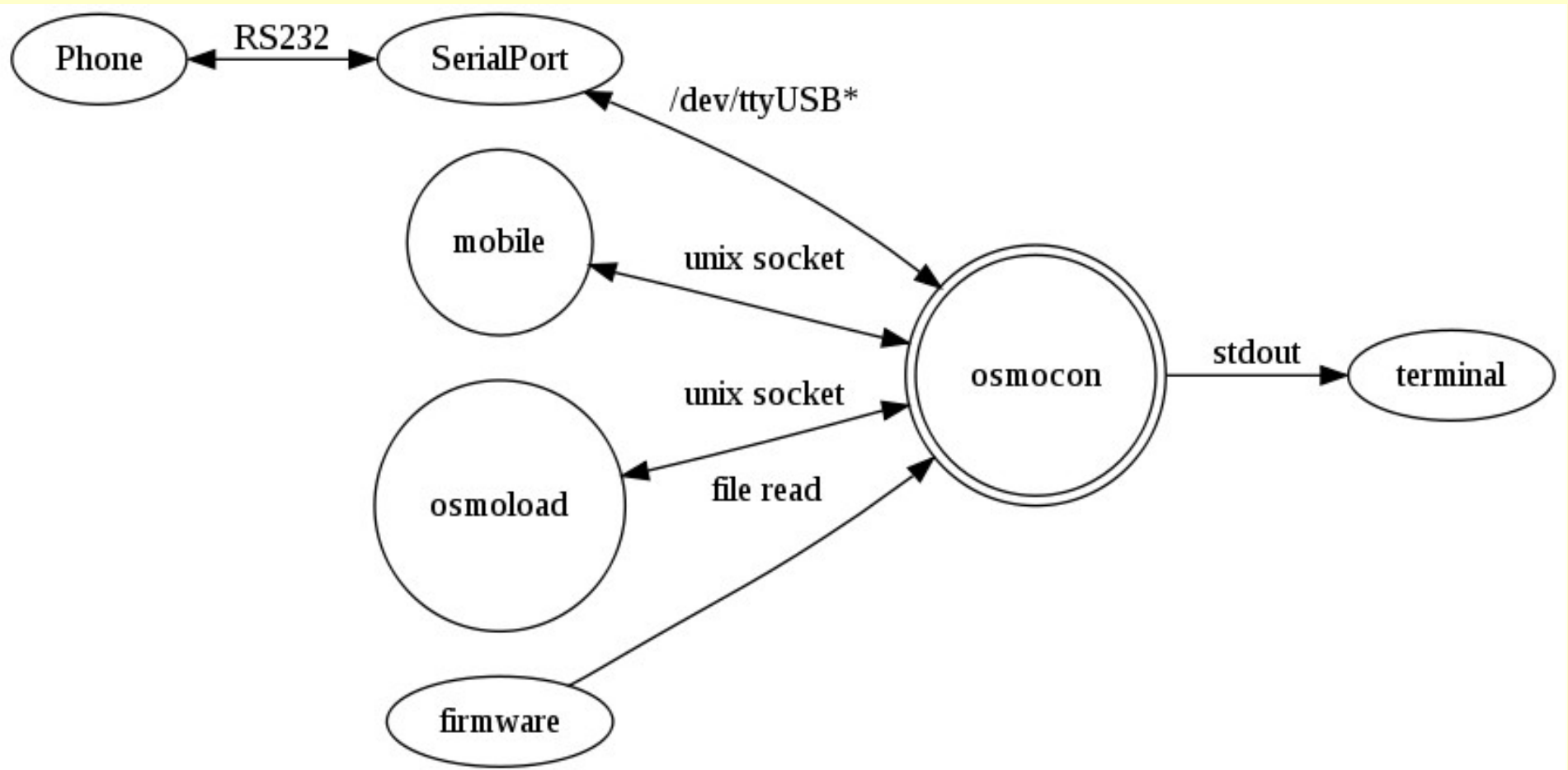
OsmocomBB

Mobilni telefon s Calypso čipovjem...



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

...in OsmocomBB strojna programska oprema



Zagon nalagalnika ROM (ang. *romloader*)

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

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

Pregled baznih postaj...

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

Terminal 0 Terminal 1 Terminal 2 Terminal 3 Terminal 4

Pregled ARFCN-jev s programom *cell_log*.

Analiza GSM prometa...

The image shows a Wireshark capture of GSM traffic. The main pane displays a list of frames with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected frame (No. 2739) is a LAPDm frame from 127.0.0.1 to 127.0.0.1, containing a DTAP Mobility Management Message Type: Location Updating Request. The details pane below shows the structure of this message, including fields like Protocol Discriminator, Sequence number, Location Updating Type, and Mobile Identity (IMSI).

Overlaid on the bottom right is a terminal window showing the output of the `ccch_scan` program. The terminal output consists of multiple lines of burst indicator messages, such as `<000c> l1ctl.c:290 BURST IND: @(708084 = 0534/00/00) (-47 dBm, SNR 255)`, and error messages like `<0001> app_ccch_scan.c:709 Burst data` and `<0001> app_ccch_scan.c:721 Error decoding data, data encrypted?`.

At the bottom of the Wireshark window, the status bar indicates "Stran 30 / 40", "Privzeto", "slovenski", and "VSTA STA".

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

Varnostni pregled slovenskih GSM omrežij

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

Uporaba šifriranja - Mobitel

The screenshot shows the Wireshark interface with the filter 'lapdm' applied. The packet list pane displays several LAPDm packets, with the 11th packet selected. The packet details pane shows the following structure:

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

The raw packet bytes are shown in hexadecimal and ASCII format, with the ASCII portion being garbled.

Algorithm identifier (gsm_a.algorithm_identifer), 1 ... Packets: 671 Displayed: 11 Marked: 0 Load time: 0:00.018 Profile: ...

Mobitel je v času pregleda uporabljal šifriranje A5/1

Uporaba šifriranja - Mobitel

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

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

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

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

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

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

Uporaba šifriranja - Mobitel

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: gsmtap Expression... Clear Apply Save

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

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

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

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

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

Uporaba šifriranja - Simobil

simobil_dokaz.pcap [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

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

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

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

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

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

Uporaba šifriranja - Simobil

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

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

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

▶ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)

▶ User Datagram Protocol, Src Port: 58444 (58444), Dst Port: gsmtap (4729)

▶ GSM TAP Header, ARFCN: 32 (Downlink), TS: 0, Channel: SDCCH/8 (5)

▶ Link Access Procedure, Channel Dm (LAPDm)

▼ GSM A-I/F DTAP - Ciphering Mode Command

▶ Protocol Discriminator: Radio Resources Management messages
DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)

▼ Cipher Mode Setting

.... ..0 = SC: No ciphering (0)

▼ Cipher Mode Response

...1 = CR: IMEISV shall be included (1)

0010 00 43 4f b1 40 00 40 11 ec f6 7f 00 00 01 7f 00 .CO.@.@.

0020 00 01 e4 4c 12 79 00 2f fe 42 02 04 01 00 00 20 ...L.y./ .B....

0030 31 ff 00 19 7f 4b 08 00 05 00 03 00 0d 06 35 10 1....K..5

0040 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b ++++++++ ++++++++

0050 2b +

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

Uporaba šifriranja - Tušmobil

Filter: Expression... Clear Apply

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

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

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

0030
0040
0050

Algorithm identifier (gsm_a.algori... = Packets: 7219 Displayed: 7219 Marked: 0 Profile: Default

Tušmobil je v času pregleda uporabljal A5/1.

Kriptoanaliza sejnega šifrirnega ključa Kc

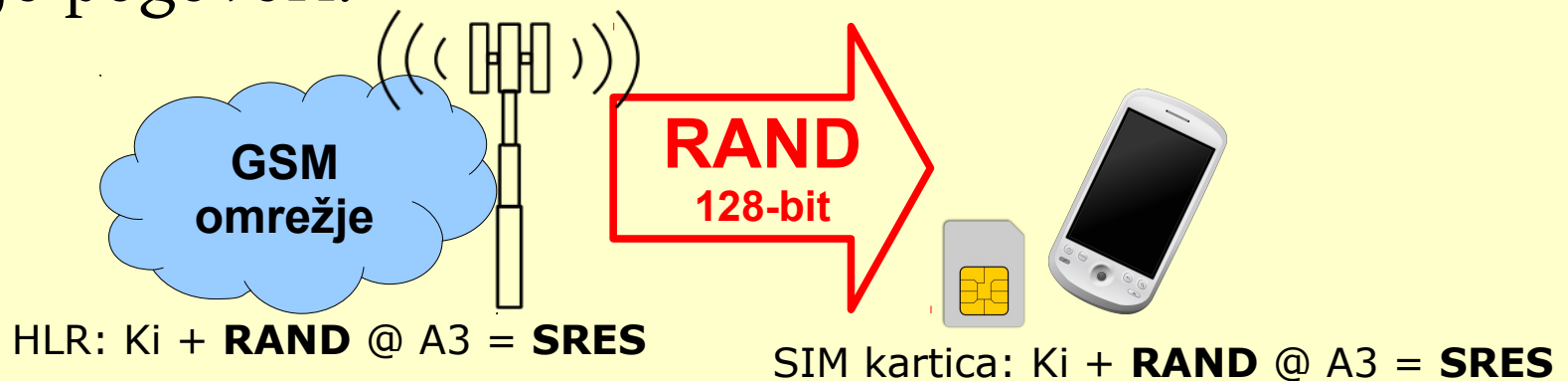
(brez posedovanja mobilnega telefona in/ali SIM kartice tarče)

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

Ustvarjanje sejnega ključa Kc

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

1.



2.



Ustvarjanje sejnega ključa Kc

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

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

4.



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

Kriptoanaliza A5/1

teorija

VSEBINA PODATKOVEGA IZBRUHA V GSM

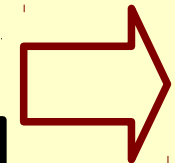
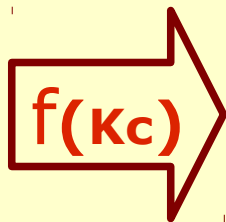
| | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 72 | FE | BC | 10 | 74 | 70 | C4 | 2B | 2B | 2B | 2B | 2B | 2B |
|----|----|----|----|----|----|----|----|----|----|----|----|----|

"ENKRATNI" KLJUČ ZA ŠIFRIRANJE TOKA PODATKOV

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

ŠIFRIRANO SPOROČILO (XOR)

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



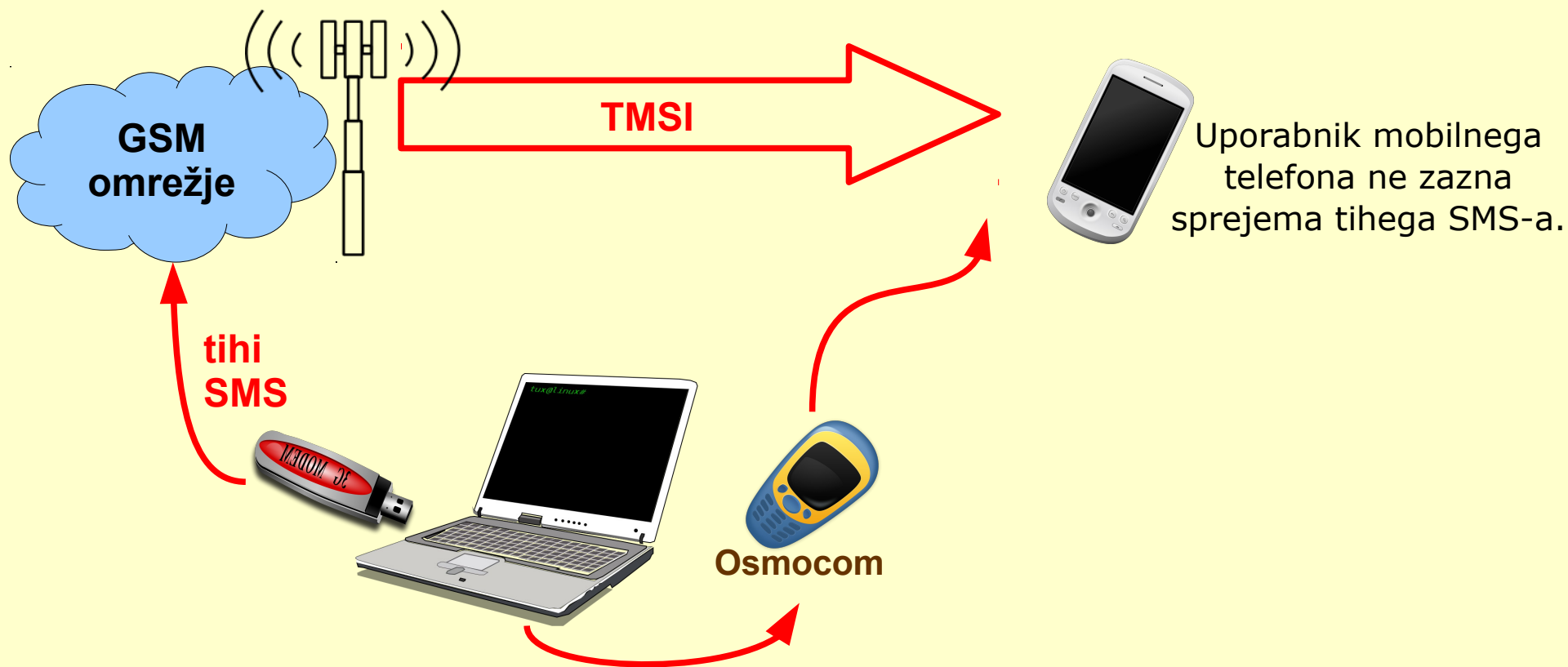
Kraken



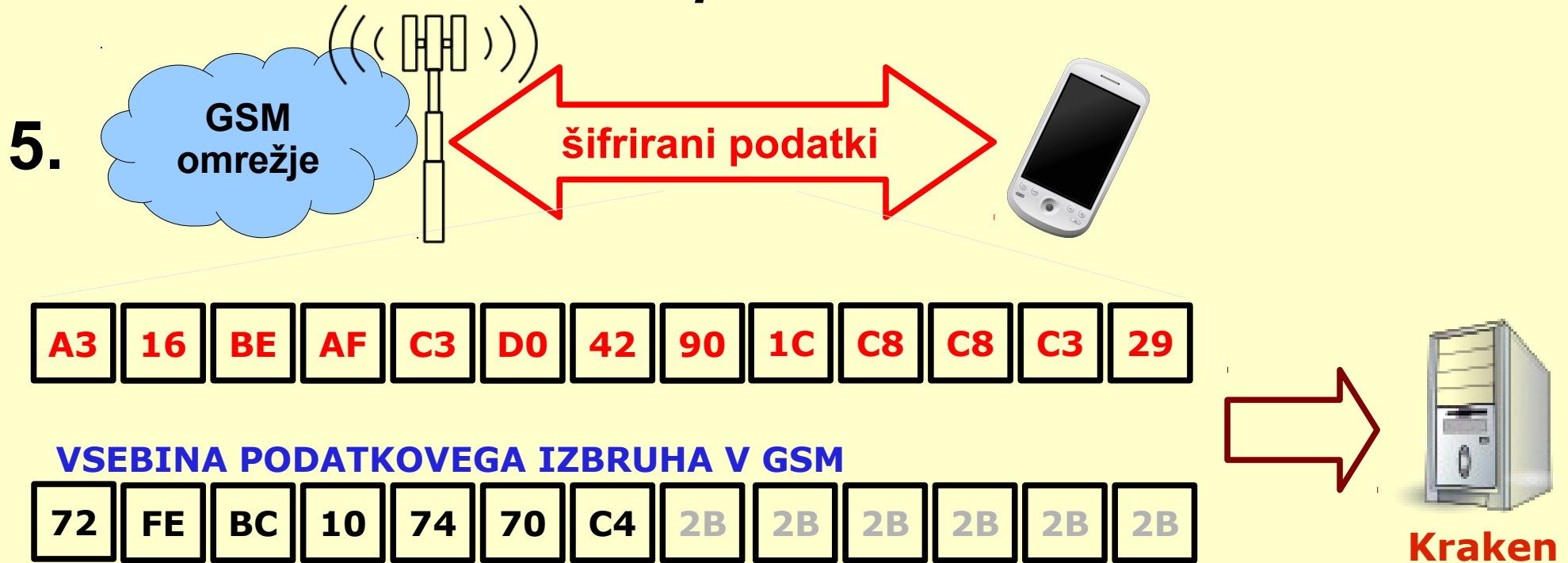
Kc

Lociranje uporabnika v mobilnem omrežju

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



Zajem in kriptanaliza A5/1 praksa



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



Navadno zapolnjevanje (*non-random padding*)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

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

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

```

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

```

Link Access Procedure, Channel Dm (LAPDm)

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

```

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

```

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

Naključno zapolnjevanje (*random padding*)

The screenshot shows the Wireshark interface with the filter 'gsmtap' applied. The packet list pane displays several packets, with packet 7647 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, IP, UDP, GSM TAP Header, and GSM A-I/F DTAP - Identity Request. A red box highlights the 'Identity Type' field, which contains the hexadecimal value 05 18 03, corresponding to the ASCII characters 'L.T.' in the hex dump below.

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

```
[Coloring Rule String: udp]
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
> User Datagram Protocol, Src Port: 48605 (48605), Dst Port: gsmtap (4729)
> GSM TAP Header, ARFCN: 104 (Downlink), TS: 1, Channel: SDCCH/8 (0)
> Link Access Procedure, Channel Dm (LAPDm)
- GSM A-I/F DTAP - Identity Request
  > Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..01 1000 = DTAP Mobility Management Message Type: Identity Request (0x18)
    0000 .... = Spare bit(s): 0
  > Identity Type
    0020 00 01 00 0d 12 79 00 21 1e 42 02 04 01 01 00 08 .....y./ .B.....l
    0030 bd 00 00 17 4c 9c 08 00 00 00 03 54 0d 05 18 03 ....L... ..T...
    0040 92 da c9 32 8d 59 71 d1 8e ce 4e 6e 35 dd 65 25 ...2.Yq. ..Nn5.e%
    0050 3d                                     1
```

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

Razbijanje A5/1 sejnega šifrirnega ključa Kc v praksi

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

Filter: `gsmstap` Expression... Clear Apply Save

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

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

Frame (81 bytes) Reassembled LAPDm (101 bytes)

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

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

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

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

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

Aplikacija *mobile*

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

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

Aplikacija *mobile*

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

Pošiljanje SMS sporočila iz aplikacije *mobile*.

Aplikacija *mobile*

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

Now start mobile application:

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

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

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

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

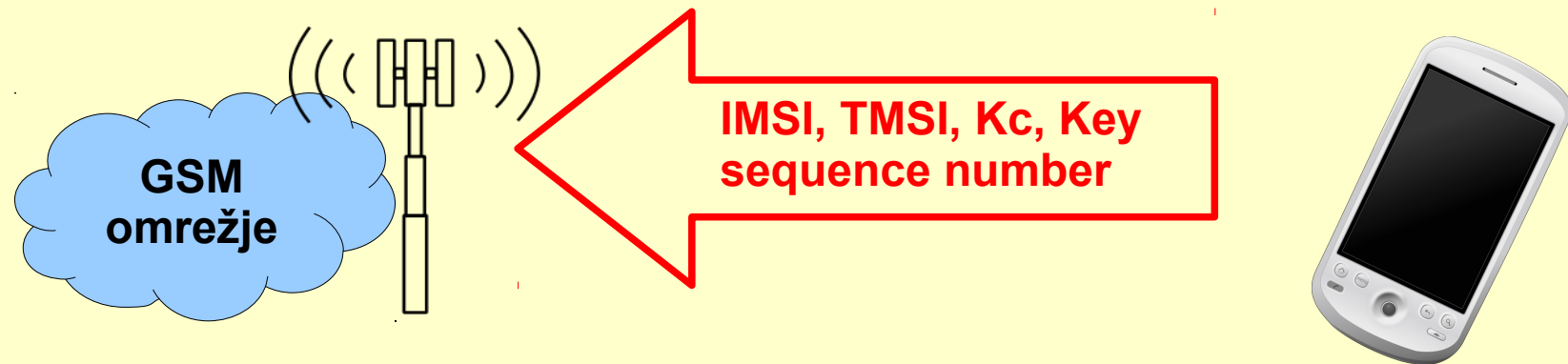
L1CTL_RESET_REQ: FULL!SIM Request (7):
SIM Response (2):
SIM Request (5):
SIM Response (28)
SIM Request (7):
SIM Response (2):
SIM Request (5):
SIM Response (17)
SIM Request (5):

ELECT (file=0x7f20)
ending APDU (class 0xa0, ins 0xa4)
received APDU (len=0 sw1=0x9f sw2=0x1a)
command successfull
ET RESPONSE (len=26)
ending APDU (class 0xa0, ins 0xc0)
received APDU (len=26 sw1=0x90 sw2=0x00)
command successfull
ELECT (file=0x6f07)
ending APDU (class 0xa0, ins 0xa4)
received APDU (len=0 sw1=0x9f sw2=0x0f)
command successfull
ET RESPONSE (len=15)
ending APDU (class 0xa0, ins 0xc0)
received APDU (len=15 sw1=0x90 sw2=0x00)
command successfull
selected file (len 9)
EAD BINARY (offset=0 len=9)
ending APDU (class 0xa0, ins 0xb0)
received APDU (len=0 sw1=0x98 sw2=0x04)
SIM Security
ending result to callback function (type=1)
<0005> subscriber.c:655 PIN is required, 3 tries left
```

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

Mobilna identiteta v mobilnem omrežju

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



Ponarejanje mobilne identitete

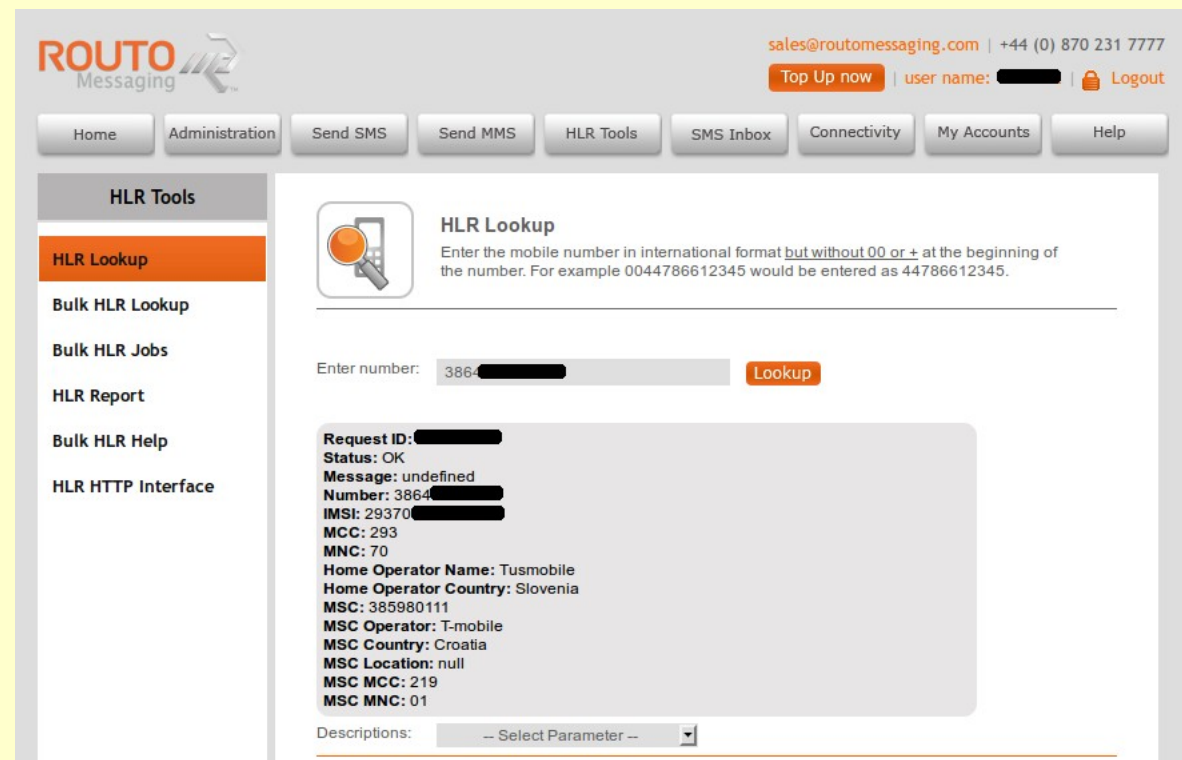
Če se Kc ne spreminja ob vsaki transakciji, je mogoče mobilno identiteto ponarediti. Najprej **identificiramo IMSI številko tarče...**

1.



HLR vpogled

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



The screenshot shows the ROUTO Messaging web interface. At the top, there is a navigation bar with buttons for Home, Administration, Send SMS, Send MMS, HLR Tools, SMS Inbox, Connectivity, My Accounts, and Help. The HLR Tools section is active, and the HLR Lookup tool is selected. The HLR Lookup tool allows users to enter a mobile number in international format (without 00 or +) to perform a lookup. The interface displays the following information:

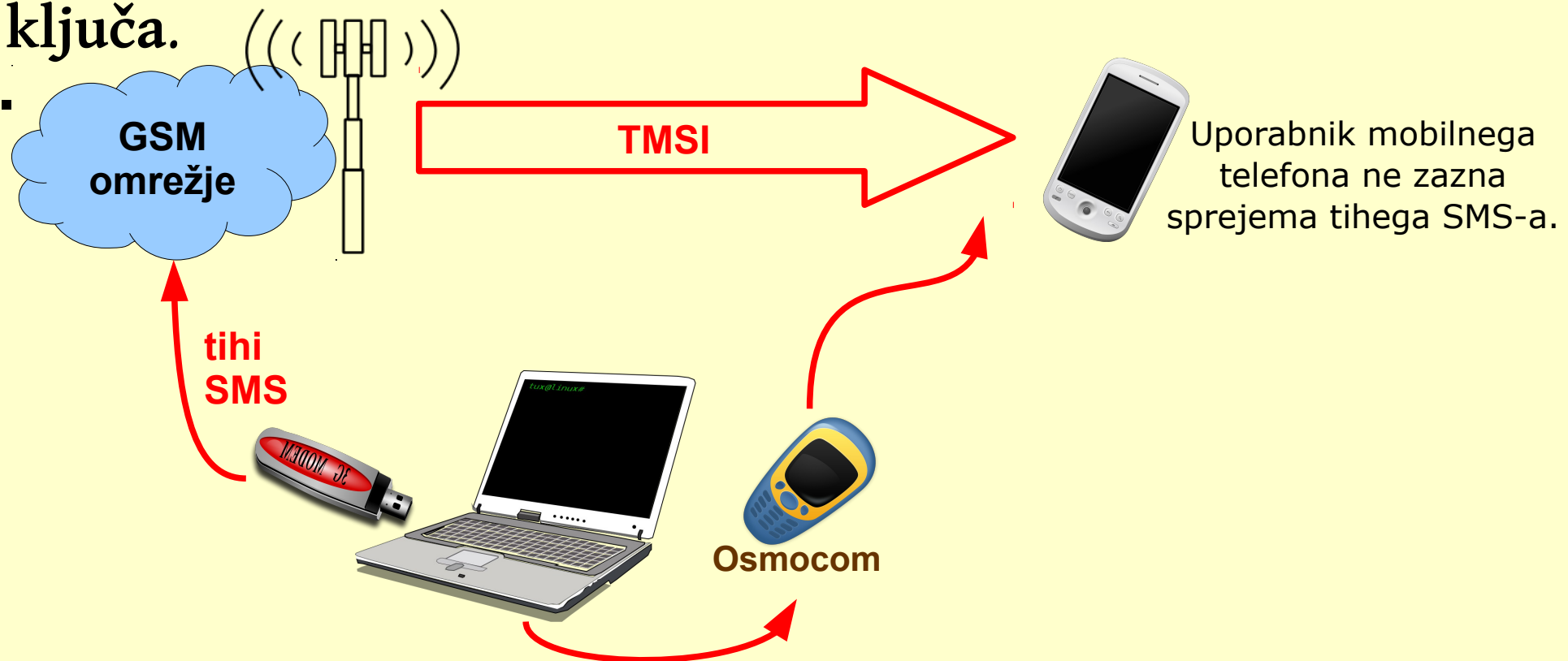
- Request ID: [redacted]
- Status: OK
- Message: undefined
- Number: 3864 [redacted]
- IMSI: 29370 [redacted]
- MCC: 293
- MNC: 70
- Home Operator Name: Tusmobile
- Home Operator Country: Slovenia
- MSC: 385980111
- MSC Operator: T-mobile
- MSC Country: Croatia
- MSC Location: null
- MSC MCC: 219
- MSC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

Below the information, there is a dropdown menu for Descriptions with the option -- Select Parameter --.

Razkritje TMSI številke

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

2.



Pridobitev Kc

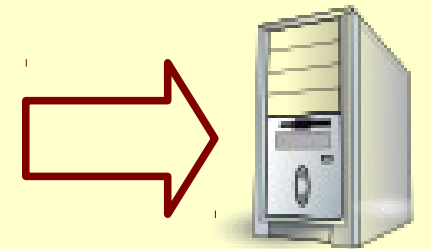
S pomočjo kriptanalize rekonstruiramo sejni šifrirni ključ Kc. Sedaj imamo vse potrebne podatke...

3.

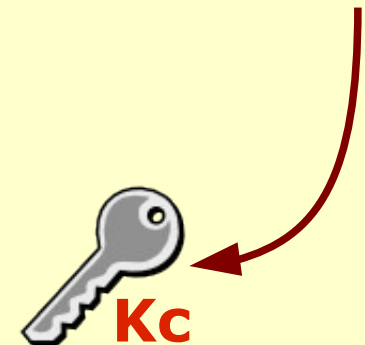
| | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| A3 | 16 | BE | AF | C3 | D0 | 42 | 90 | 1C | C8 | C8 | C3 | 29 |
|----|----|----|----|----|----|----|----|----|----|----|----|----|

VSEBINA PODATKOVEGA IZBRUHA V GSM

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



Kraken



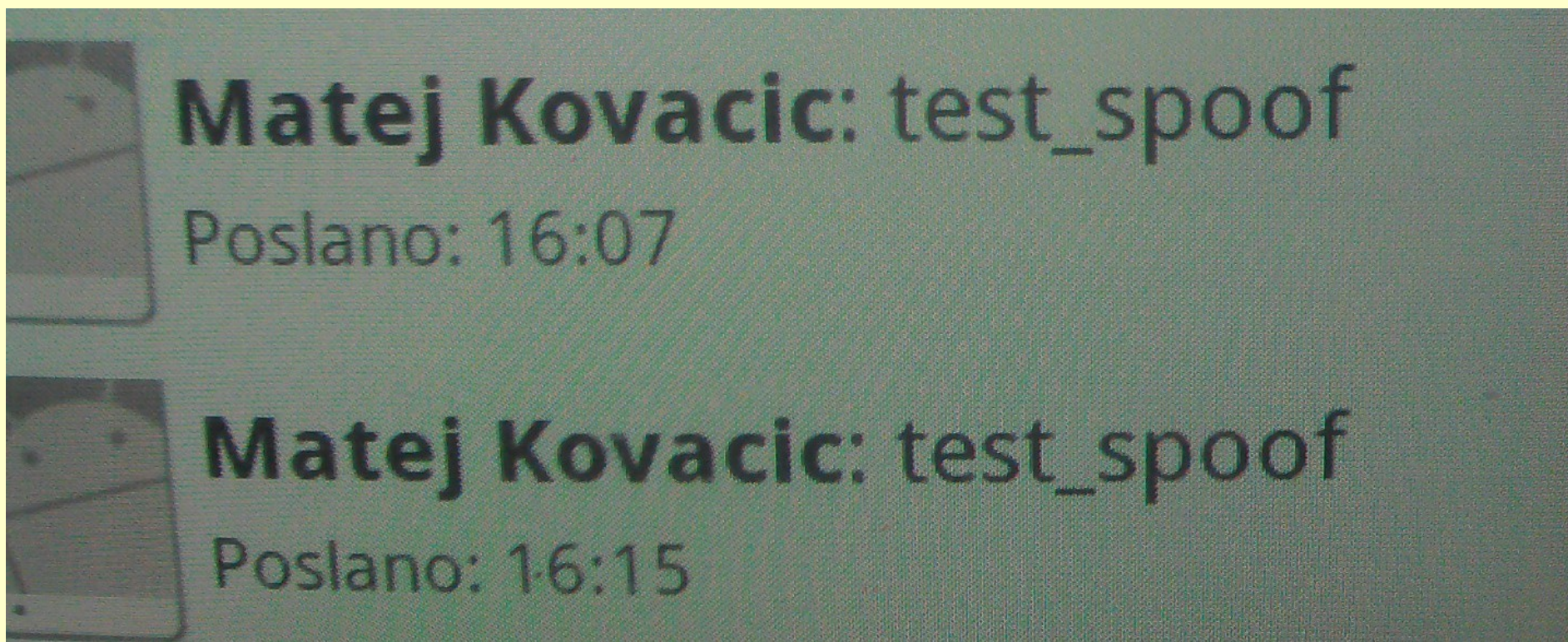
Kc

"SIM spoof"

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

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

Ponarejanje mobilne identitete



Dve SMS sporočili poslani s pomočjo ponarejene mobilne identitete.
Na podoben način je bilo mogoče ponarejati tudi glasovne klice.

[video]

**Kaj to pomeni za obvezno hrambo prometnih
podatkov? In kaj za zvočne prisluhe telefonskih
pogovorov?**

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

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

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

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

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

**Operaterji so svoja omrežja nadgradili.
Smo sedaj varni?**

Pravzaprav ne. Zakaj?

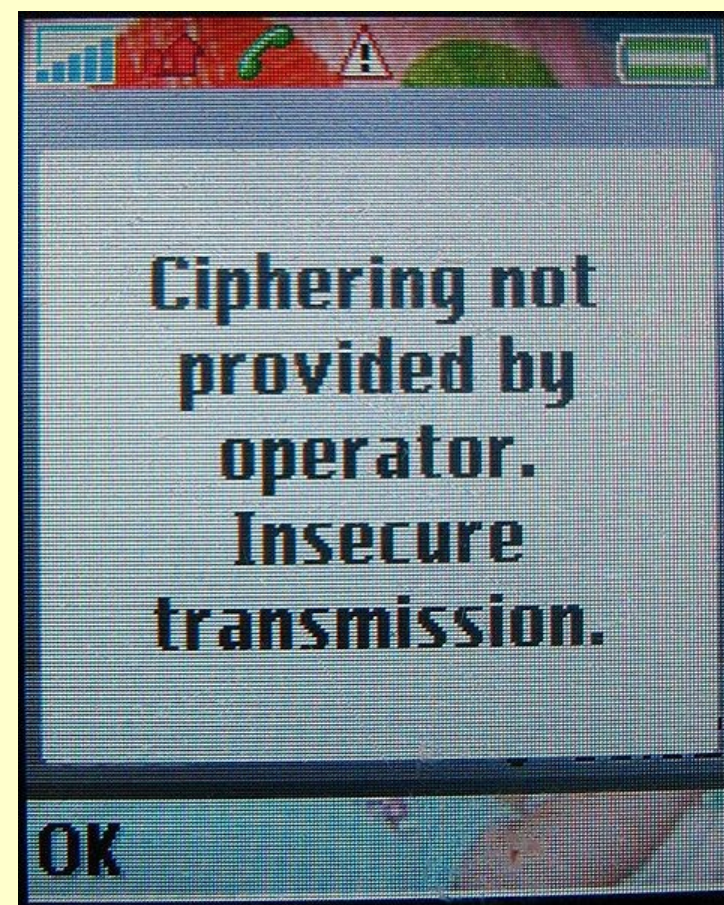
- Pošiljanje SMS sporočil s spremenjeno identifikacijo ter klicanje s spremenjeno identifikacijo je še vedno mogoče.
 - Z nekaj spretnosti so taki klici še vedno težko izsledljivi.
- Prestrezanje komunikacij je še vedno mogoče (kljub A5/3).
- Verjetno bi bilo še vedno mogoče izvajati ponarejanje mobilne identitete.
- V GSM omrežju obstajajo še nekatere druge ranljivosti.
- Na varnosti GSM tehnologije temelji tudi varnost nekaterih drugih rešitev.

Problem: mobilno omrežje se ne avtenticira mobilnemu telefonu

- GSM omrežje je zasnovano tako, da se morajo mobilni telefoni avtenticirati omrežju. Vendar pa se po drugi strani mobilno omrežje **ne** avtenticira telefonu.
- Prevod: mobilni telefon ne ve v katero mobilno omrežje je povezan.
- Posledica: mogoč je napad s tim. “IMSI-catcherjem”, posebno napravo, ki se v omrežju predstavi kot (lažna) bazna postaja. Ker mobilni telefon ne ve, da je ta bazna postaja lažna, se – če ima dober signal, in če uporabnik nima onemogočene samodejne izbire omrežja - poveže nanjo. Mogoči so tudi drugi napadi, s katerimi lažna bazna postaja mobilni telefon “prepriča”, da se vedno poveže nanjo.

Problem: mobilno omrežje se ne avtenticira mobilnemu telefonu

- Ko je mobilni telefon povezan na lažno bazno postajo, mu le-ta lahko ukaže izklop šifriranja.
- Vendar pa GSM standard priporoča ("*should*") obveščanje uporabnika kadar komunikacija ni šifrirana (3GPP Rel.9 TS 33.102-920 "3G Security Architecture" 5.5.1 Visibility, ciphering indicator feature - 3GPP TS 22.101")



Problem: mobilno omrežje se ne avtenticira mobilnemu telefonu

- Vendar pa se to obvestilo ne prikaže, če je tako nastavljeno na SIM kartici.

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: mobilno omrežje se ne avtenticira mobilnemu telefonu



Nekateri mobilni telefoni obvestilo izpišejo slabo vidno, nekateri pa ga sploh ne izpišejo.

IMSI Catcher lahko kupijo...


 REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE
 Štefanova ulica 2, 1501 LJUBLJANA
 Telefon: 01 428 40 00; telefaks: 01 428 47 33
 E-pošta: gp.mnz@gov.si; http://www.mnz.gov.si

Številka: 029-34/2010/14 (2223-01)
 Datum: 17-06-2010

**MEDRESORSKA KOMISIJA
 ZA IZDAJO SOGLASIJ ZA IZVEDBO
 OBRAMBNIH IN ZAUPNIH NAROČIL**

Ministrstvo za obrambo
 Vojkova cesta 59
 1000 Ljubljana

sekretar komisije

ZADEVA: Vloga za soglasje k izvedbi naročila na podlagi Uredbe o obrambnih in zaupnih naročilih*1

V skladu s 5. členom Uredbe o obrambnih in zaupnih naročilih (Uradni list RS, št. 80/07), ki določa, da mora naročnik za izvedbo naročila po navedeni uredbi predhodno pridobiti soglasje medresorske komisije, imenovane s strani Vlade Republike Slovenije, vas prosimo za soglasje k izvedbi sledečega zaupnega naročila:

1. Naziv ter naslov naročnika, ki bo izvedel naročilo po Uredbi o obrambnih in zaupnih naročilih:

Ministrstvo za notranje zadeve, Policija, Štefanova 2, 1501 Ljubljana

2. Predmet naročila:

Nadgradnja sistema za ~~varnostno pregrado s~~

PREMI%C4%8CNINEdo2013.xls - LibreOffice Calc

Datoteka Uredi Pogled Vstavi Oblika Orodja Podatki Okno Pomoč

Arial 10

C181 f(x) Σ = Sistem za motenje in nadzor mobilne telefonije

| | A | B | C | D | E | F |
|---|---|--------------------|--|-------------------------|-----------------------------|---|
| 1 | Preglednica 5: Načrt pridobivanja premičnega premoženja - leto 2013 | | | | | |
| 2 | | | | | | |
| 3 | Upravljenec | Zaporedna številka | Vrsta premičnega premoženja | Okvirni obseg premičnin | Predvidena sredstva (v EUR) | Ekonomska utemeljenost |
| | 181 | 113 | Sistem za motenje in nadzor mobilne telefonije | 1 | 238.400,00 | Nadzor in motenje mobilne telefonije - naprava je nepogrešljiv pripomoček pri opravljanju protipristuškovalnih pregledov. |
| | 182 | 114 | Sistem za motenje radijskih naprav | 1 | 97.236,00 | Onemogočanje komunikacije naprav, ki komunicirajo preko radiofrekvenčnega spektra - naprava je primerna za motenje v primeru sestankov zaupne narave in pri izvajanju policijskih pooblastil. |
| | 183 | 115 | Varnostna pregrada | 1 | 64.000,00 | Zaščita komunikacije z Internetom - potrebna je varnostna pregrada s |

Delovni list 1 / 2 PageStyle_Preglednica 5 STA Vsota=0 100%

...ali pa si ga izdelamo sami

```
root@bt: ~/sylvainbts/osmocom-bb/src/host/osmocon.77x21
Charging at 239 LSB (204 mA).
BCICL2=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).
BCICL2=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

root@bt:~/openBts/public/smqueue/trunk/smqueue 77x21
root@bt:~/openBts/public/smqueue/trunk/smqueue# ./smqueue
ALERT 3074709728 smqueue.cpp:2421:main: smqueue (re)starting
smqueue logs to syslogd facility LOCAL7, so there's not much to see here

root@bt:~/openBts/public/openbts/trunk/apps 77x20
<0011> trx.c:512 TRX Data 25706:0:0:816a80aa0221546952a45085401000
<0011> trx.c:512 TRX Data 25707:0:0:018a122916244ae0428548042a4480
<0011> trx.c:512 TRX Data 25708:0:0:14a01404481448700a10a010804aa0
<0011> trx.c:512 TRX Data 25709:0:0:4421420408540070a810001a212280
<0011> trx.c:190 TRX CLK Indication 25706
<0011> trx.c:512 TRX Data 25757:0:0:8062948a52a104e0402112806004a0
<0011> trx.c:512 TRX Data 25758:0:0:118a5288440000e102854a018a1600
<0011> trx.c:512 TRX Data 25759:0:0:408904254000607400058000200220
<0011> trx.c:512 TRX Data 25760:0:0:44a542052054286588022012a16200
<0011> trx.c:190 TRX CLK Indication 25757
<0011> trx.c:512 TRX Data 25808:0:0:82c074272b9d407e30b44143d79a20
<0011> trx.c:512 TRX Data 25809:0:0:618bfbb007ffc0f38b52440fad7c70
<0011> trx.c:512 TRX Data 25810:0:0:278f25f0c41b906604be6288b10310
<0011> trx.c:512 TRX Data 25811:0:0:a51bec5f9010e6fe6a32f311c21810
<0011> trx.c:190 TRX CLK Indication 25808
<0011> trx.c:512 TRX Data 25859:0:0:a847551a314dc060907c410b055130
<0011> trx.c:512 TRX Data 25860:0:0:22974400ea1647e9ab7e0003df5460
<0011> trx.c:512 TRX Data 25861:0:0:042f958b02511c670ff15001178680
<0011> trx.c:512 TRX Data 25862:0:0:9581ac70181285f07a0b57d681fe70
```

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>>.

...ali pa si ga izdelamo sami



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 detektor...



```
matej@cryptopia: ~/catchercatcher/osmocombb/src/host/layer23/src/mobile
matej@cryptopia: ~/osmocombb/src/host/layer23/src/mobile
OsmoComBB# show catcher
Catcher status for MS '1'
link establishment
  rach sent: 2
  paging: 0
  imm_ass: 1
  assign: 0
  handover: 0
  release: 1
  tune: 1
  failure: 0
  current: 0
  high pwr: 0.00
cipher mode
  request: 1
  response: 1
  no cipher: 0
  no IMEISV: 0
  first alg: A5/1
  last alg: A5/1
cell monitoring
  camped: 0
  MCC: 293 (293, 0)
  MNC: 40 (40, 0)
  LAC:
  CID:
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
```

...pa obstaja samo za Osmocom telefone

(FemtoCatcher pa za Verizonove mobilnike).

Nekateri drugi napadi na mobilno telefonijo

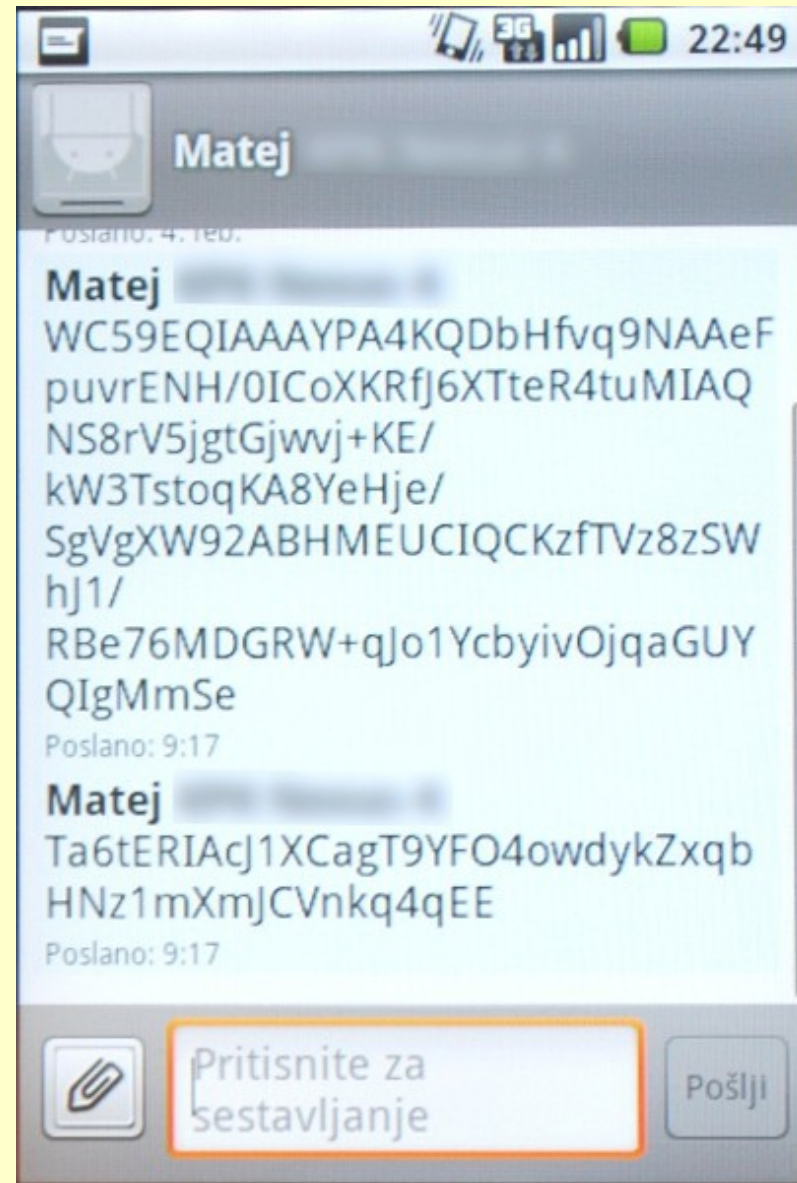
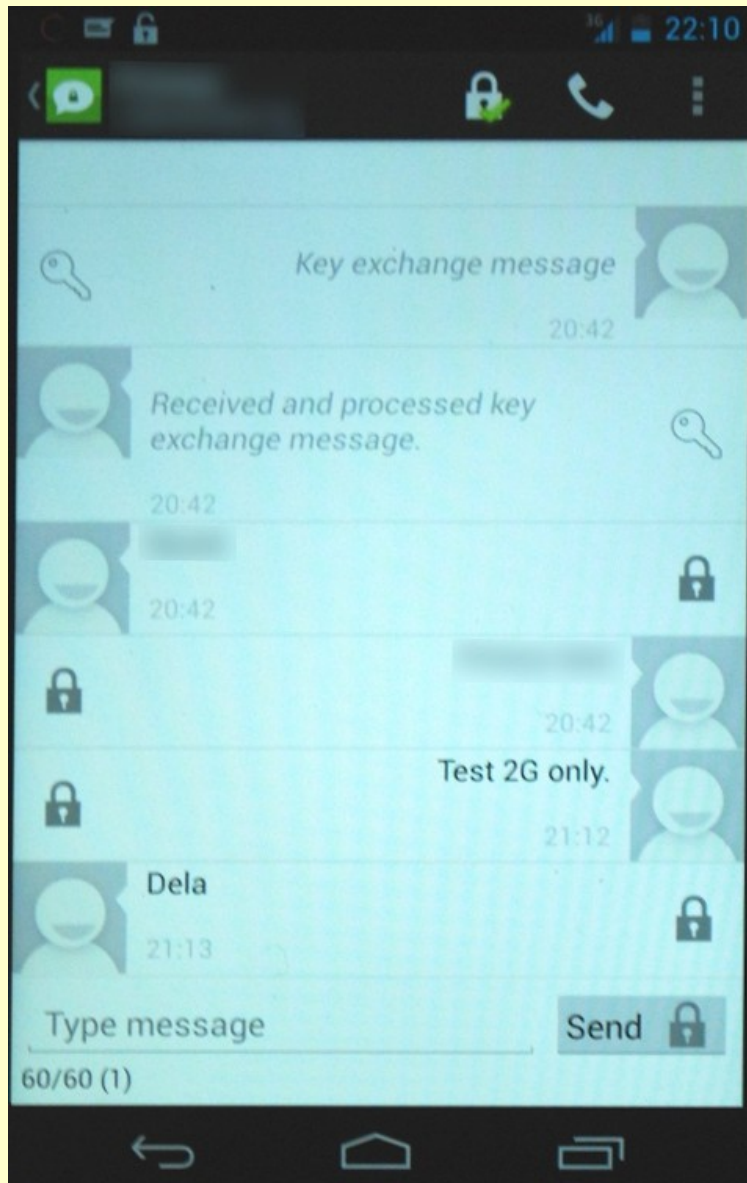
- **Odklop mobilnega telefona iz omrežja:** napadalec, ki pozna IMSI in TMSI številko tarče, le-to lahko odklopi iz omrežja s pomočjo [REDACTED].
- **Prenehanje delovanja (izklop) omrežja:** če napadalec v manj kot [REDACTED] pošlje več [REDACTED] paketkov kot ima bazna postaja [REDACTED], omrežje preneha delovati. Gre za tim. [REDACTED] poplavljanje, posledica pa je prenehanje delovanja omrežja (tim. Denial Of Service napad).

Rešitve?

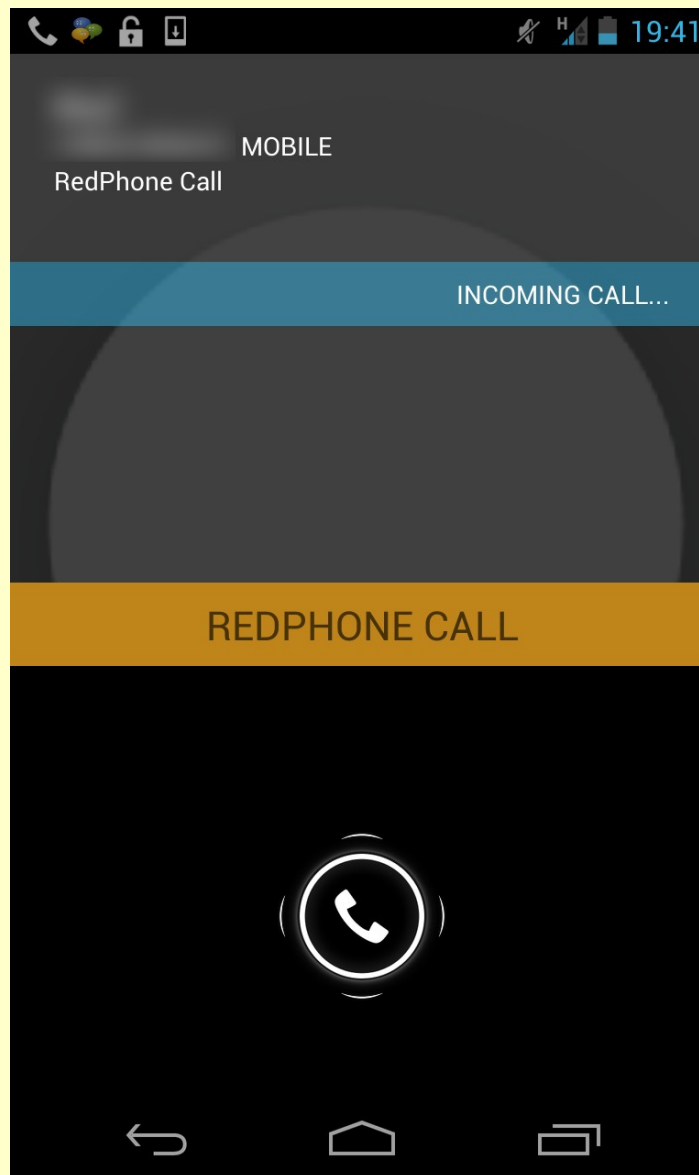
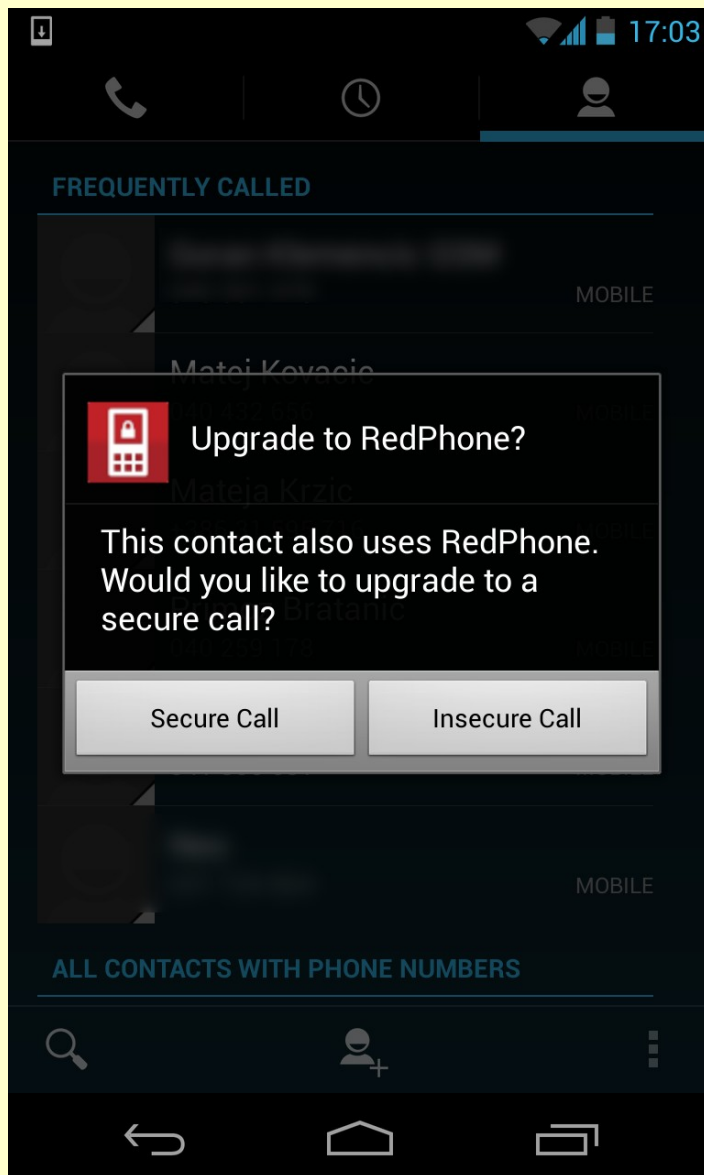
Šifrirane digitalne komunikacije

- Šifrirane digitalne komunikacije so že realnost!
- Tehnologije so **prosto dostopne**.
- Omogočajo šifriranje vsebine komunikacij **od začetne do končne točke** (tim. *end-to-end*).
 - Posledica: prisluškovanje, tudi tim. zakonito **ni več mogoče**.
- Omogočajo praktično **nezlomljivo zaščito** (uporaba najsodobnejših šifrirnih mehanizmov) ob enostavni uporabi.
- Trend: skrivanje oz. **onemogočenje beleženja prometnih podatkov**.

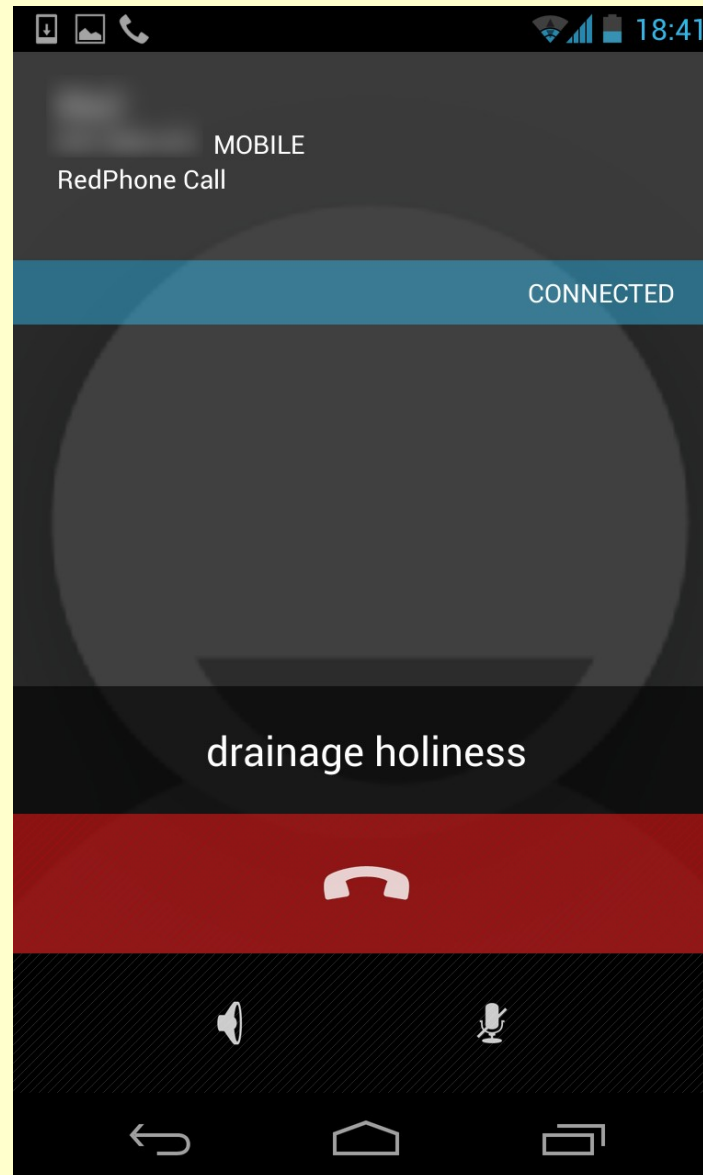
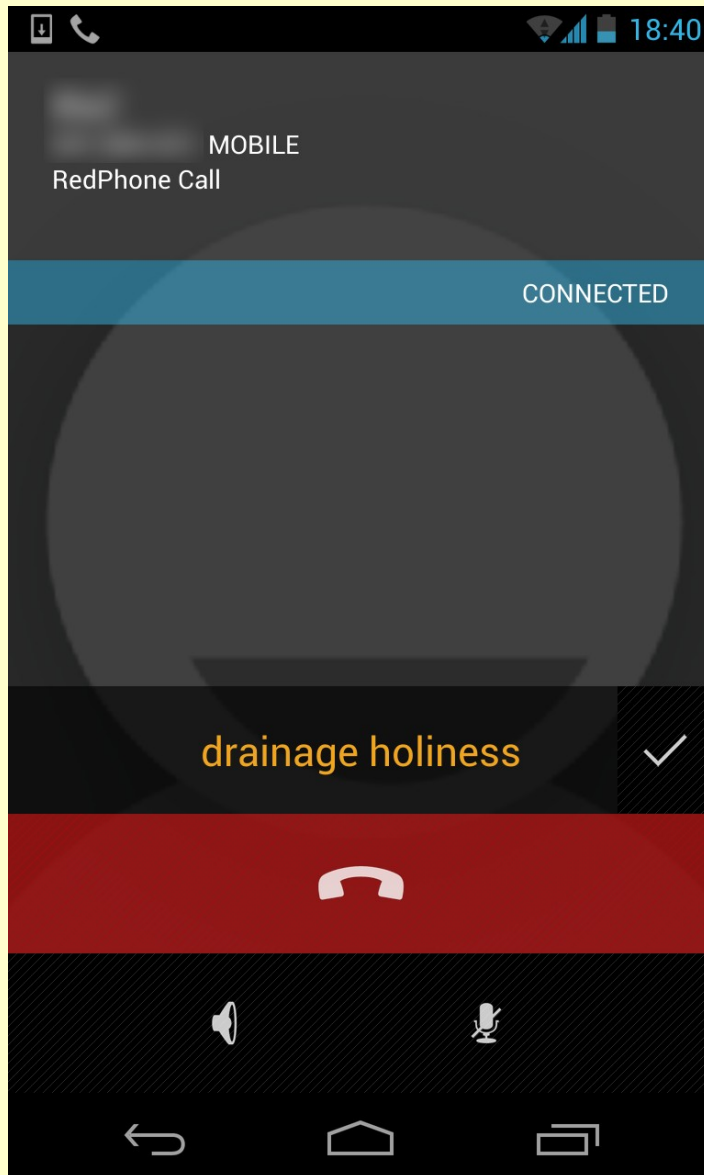
Šifrirana SMS sporočila: TextSecure



Šifrirani telefonski pogovori: RedPhone



Šifrirani telefonski pogovori: RedPhone



Kako je slišati nešifriran telefonski pogovor (IP telefonija)?

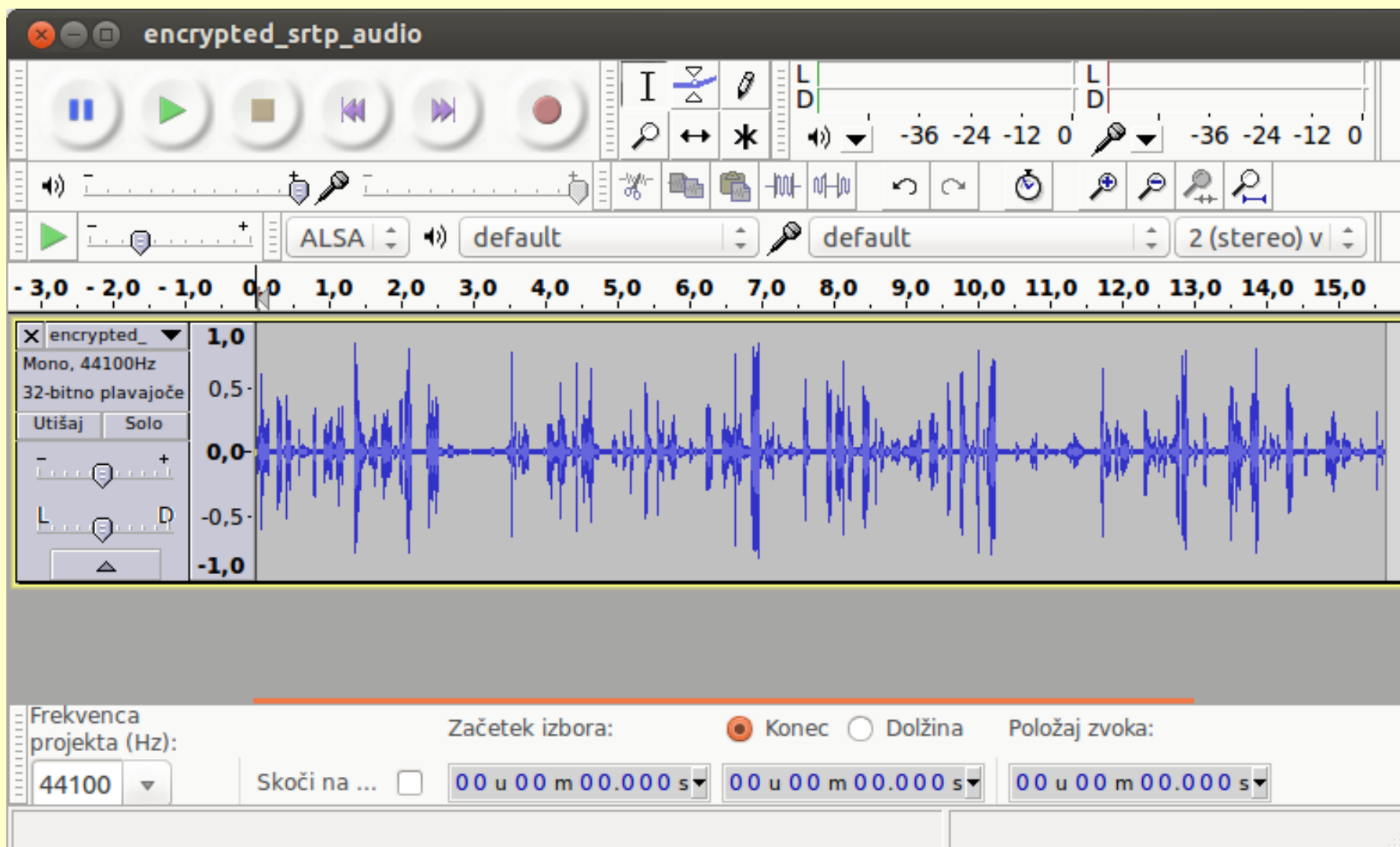
The image shows a Wireshark interface with several windows open. The main window displays a list of captured packets, with a filter set to 'sip'. The packet list shows several SIP and SIP/SDP messages. A red box highlights a SIP message with status '100 Trying'. Another red box highlights a SIP message with status '200 OK'. Below the packet list, a packet details pane shows the structure of a SIP message, with a red box highlighting the 'To' field containing '212.1'. A 'VoIP Calls' window is open, showing a table of detected calls. A 'VoIP - RTP Player' window is also open, displaying a waveform of the audio stream. The RTP player window shows two calls: one from 172.16.0.116:5062 to [redacted] with a duration of 64.04s, and another from [redacted] to 172.16.0.116:5062 with a duration of 64.57s. The RTP player window also shows a 'Jitter buffer [ms]' set to 50 and a 'Use RTP timestamp' checkbox. The bottom status bar of the main window shows 'Packets: 9799 Displayed: 9799 Marked: 0 Profile: Default'.

| No. | Time | Source | Destination | Protocol | Info |
|-----|-----------|--------|-------------|----------|---|
| 69 | 14.865457 | 153.5 | 212.1 | SIP/XML | Request: PUBLISH sip: [redacted]@212.1 |
| 72 | 16.867222 | 153.5 | 212.1 | SIP/XML | Request: PUBLISH sip: [redacted]@212.1 |
| 82 | 23.453253 | 153.5 | 212.1 | SIP/SDP | Request: INVITE sip:015805373@212.1, with |
| 83 | 23.461385 | 212.1 | 153.5 | SIP | Status: 100 Trying |
| 84 | 23.466803 | 212.1 | 153.5 | SIP | Status: 401 Unauthorized |
| | | | | SIP | Request: ACK sip:015805373@212.1 |
| | | | | SIP/SDP | Request: INVITE sip:015805373@212.1 with |
| | | | | SIP | Status: 100 Trying |
| | | | | SIP | Status: 200 OK |
| | | | | SIP | Request: CANCEL sip:015805373@212.1 |
| | | | | SIP | Status: 487 Request Cancelled |
| | | | | SIP | Request: ACK sip:015805373@212.1 |

| 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 Kovacic" <sip:[redacted] | [redacted] | SIP | 14 | COMPLETE | |

[Demo]

Kako je slišati šifriran telefonski pogovor?

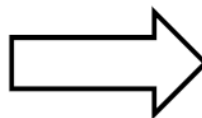


[Demo]

Prometni podatki RedPhone klicev

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 |

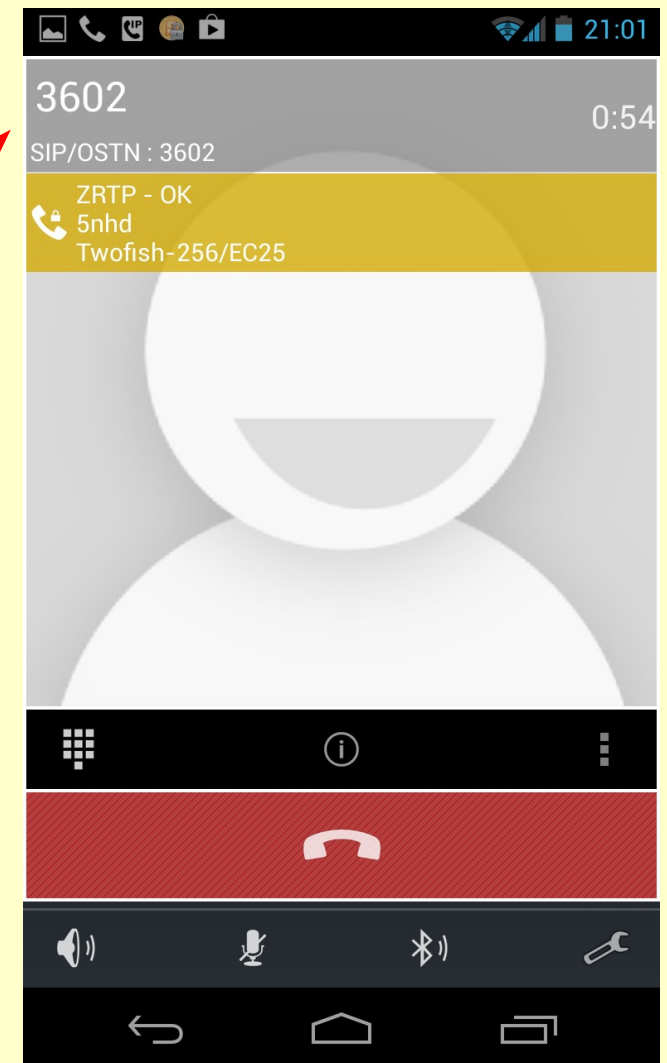
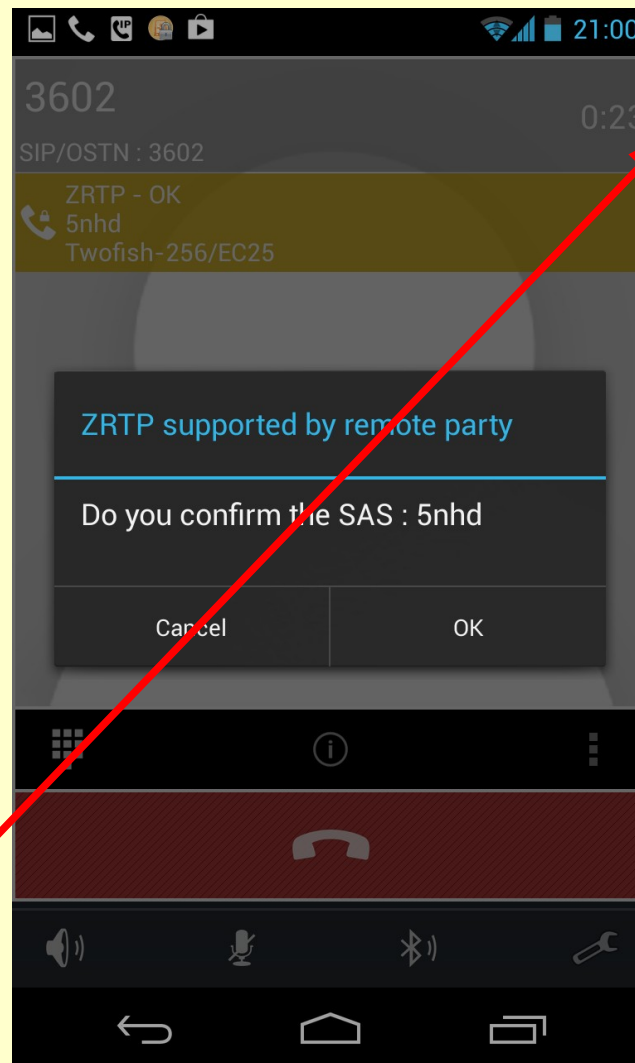
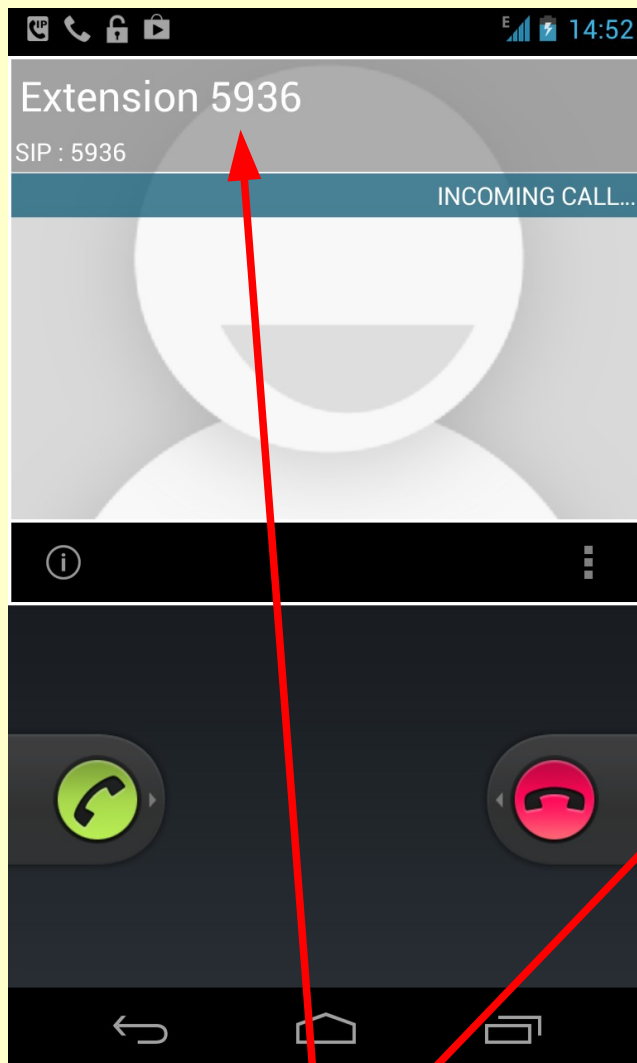


| tip klica | klicana oseba | datum in čas | trajanje |
|-----------|---------------|-------------------------|----------|
| RP klic | Nemčija | Jun 1, 2013 12:52:36 PM | 37 |
| RP klic | Nemčija | Jun 1, 2013 12:53:28 PM | 23 |
| RP klic | Nemčija | Jun 1, 2013 12:54:40 PM | 22 |
| RP klic | Nemčija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

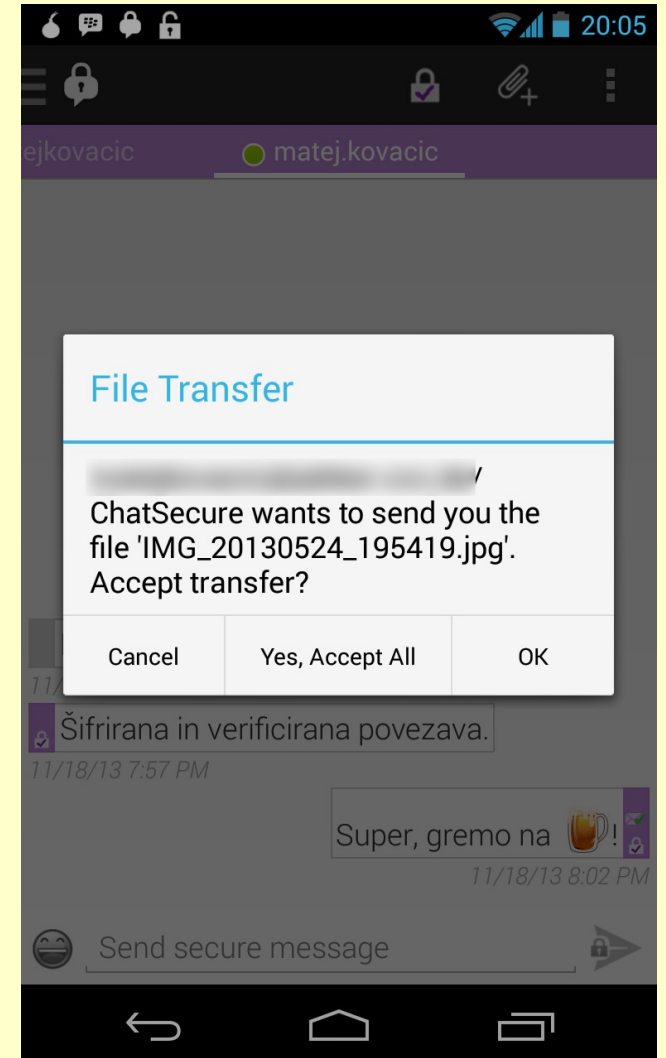
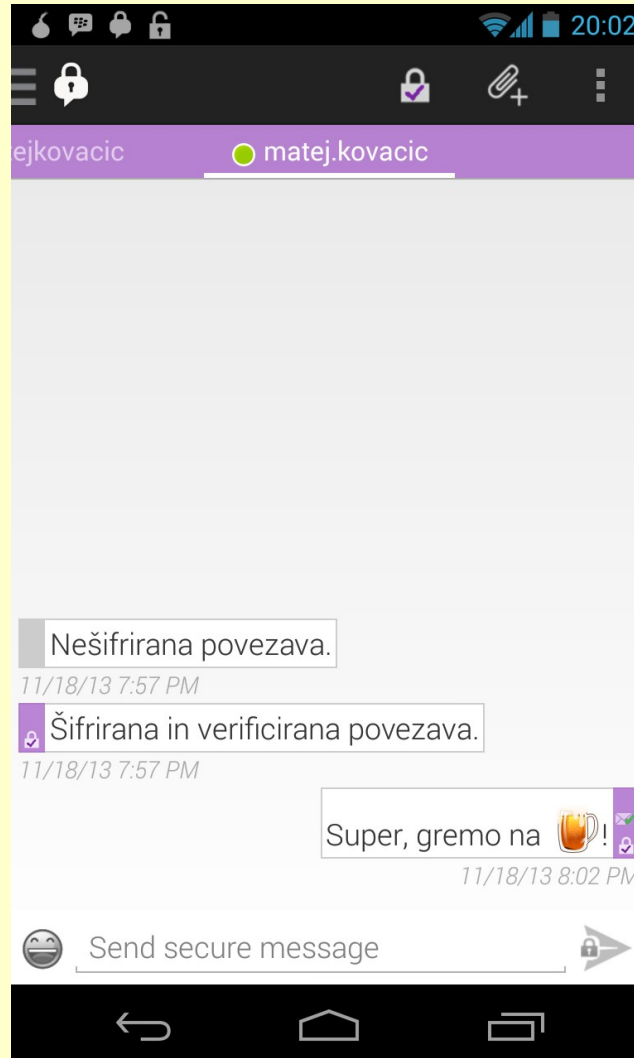
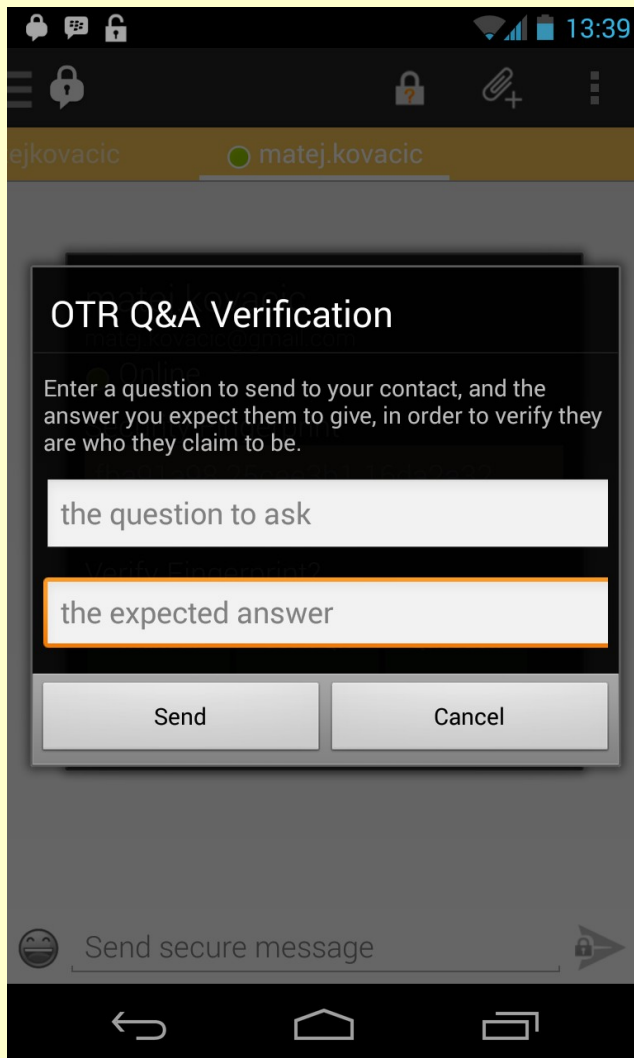
| tip klica | klicana oseba | datum in čas | trajanje |
|-----------|---------------|-------------------------|----------|
| RP klic | Slovenija3 | Jun 2, 2013 10:47:14 AM | 11 |
| RP klic | Slovenija3 | Jun 2, 2013 10:47:52 AM | 64 |
| RP klic | Slovenija3 | Jun 2, 2013 10:49:03 AM | 102 |
| RP klic | 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 |

Šifrirana IP telefonija: CSipSimple



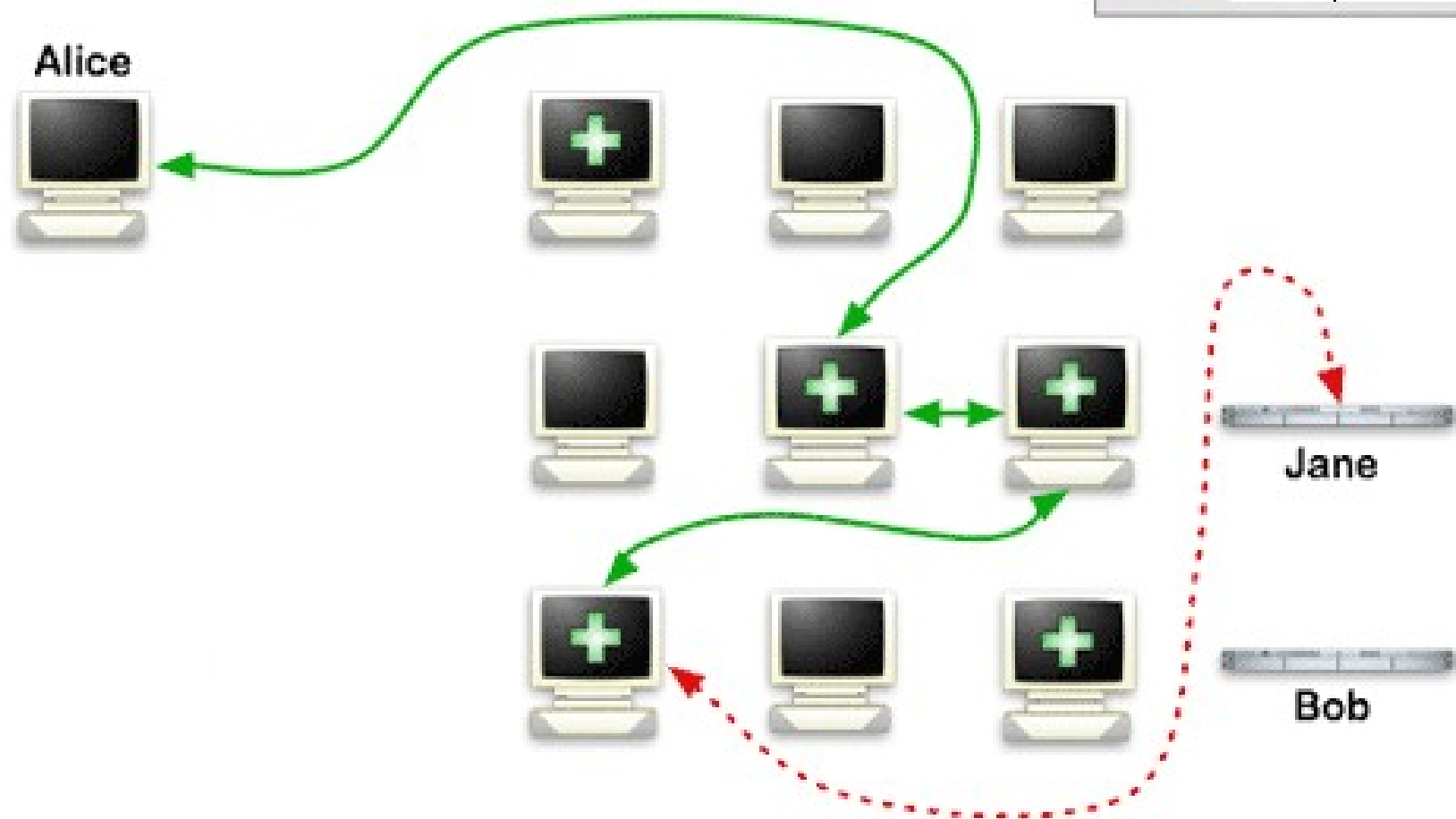
Prometni podatki?

Šifrirana hipna sporočila: ChatSecure

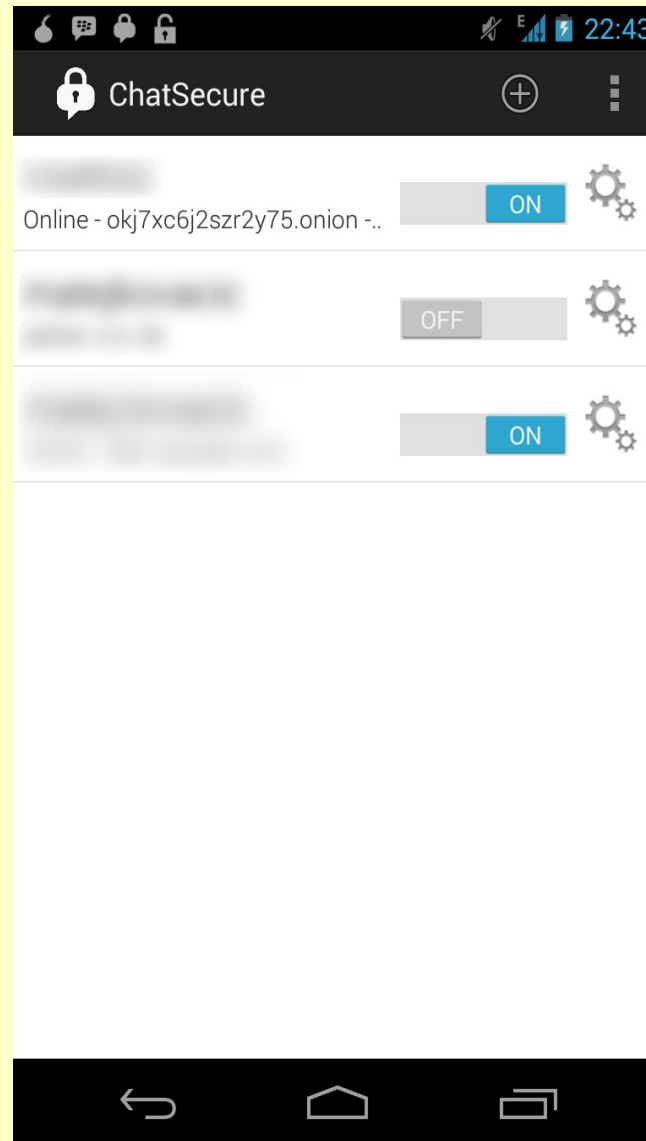
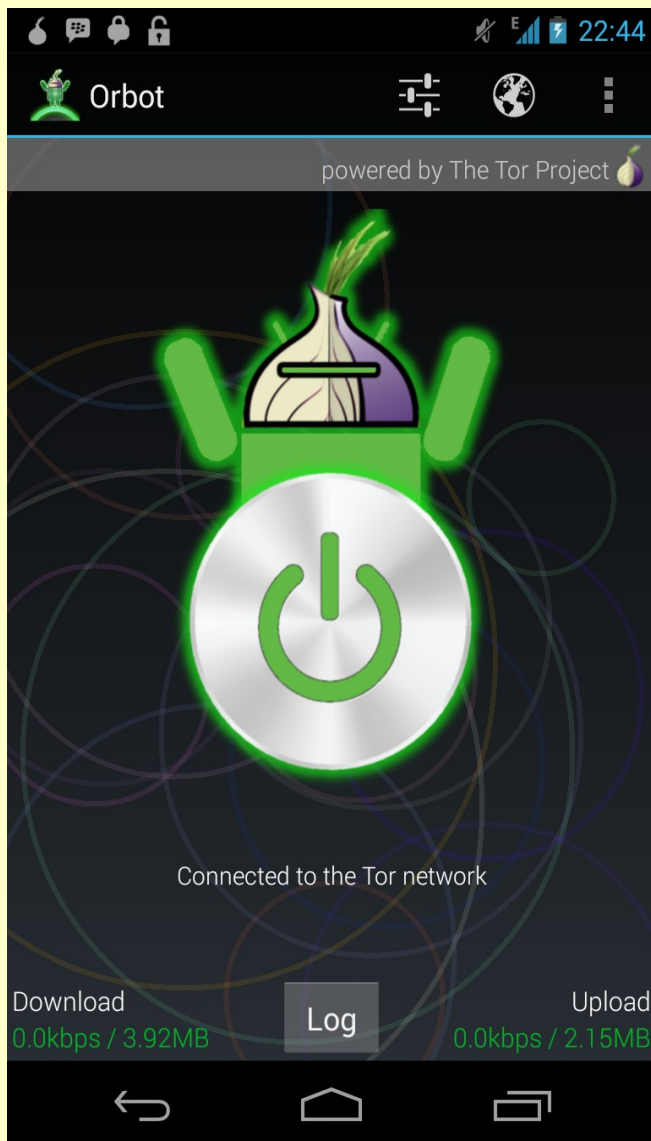


Anonimizacija...

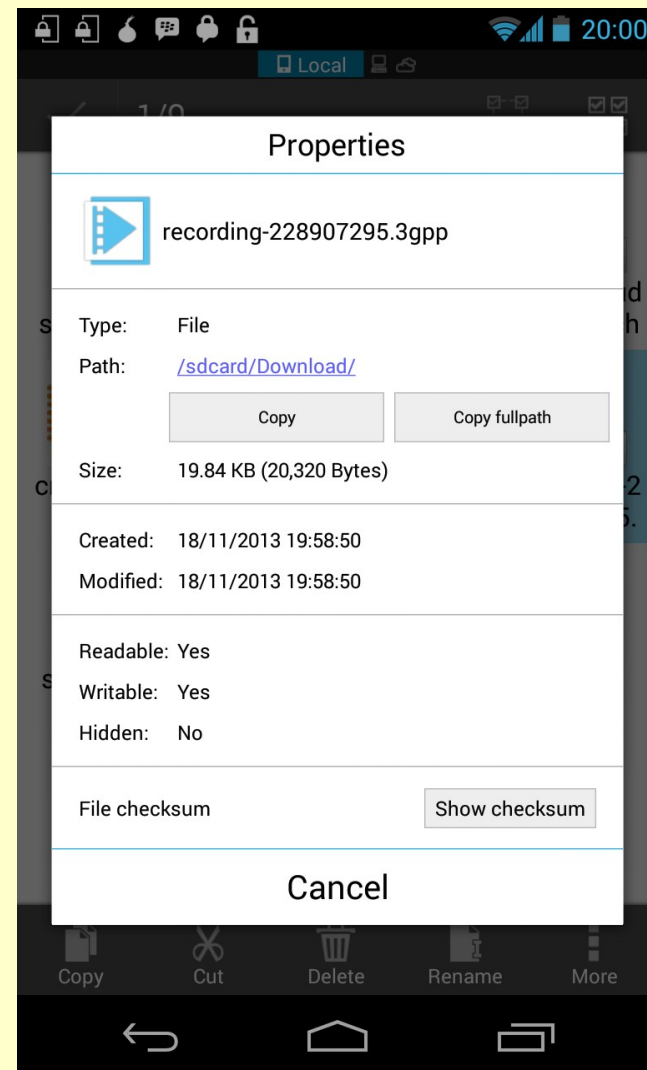
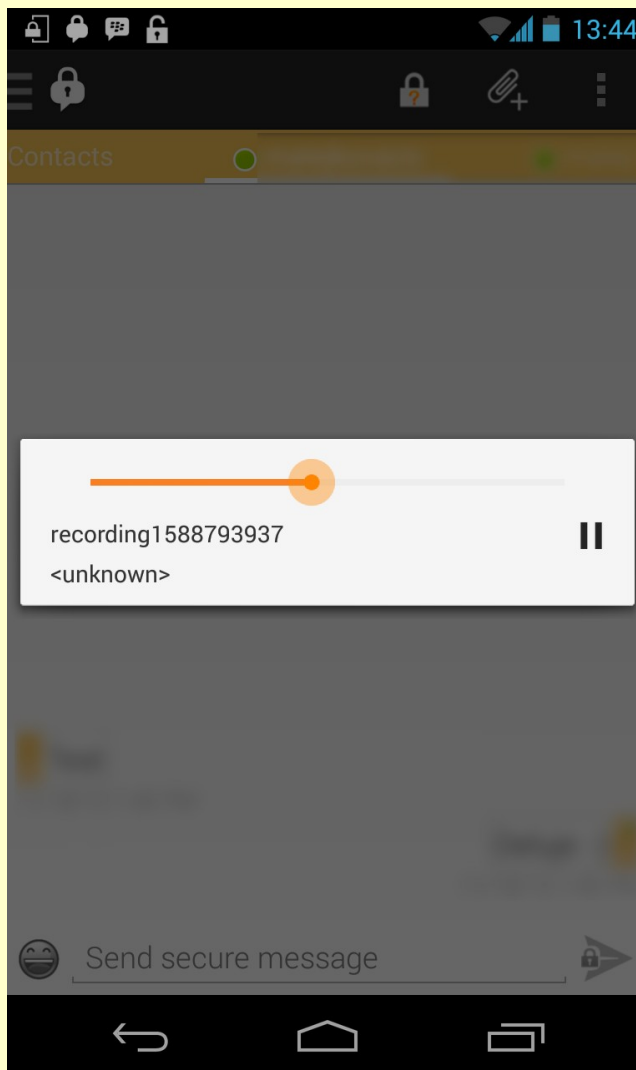
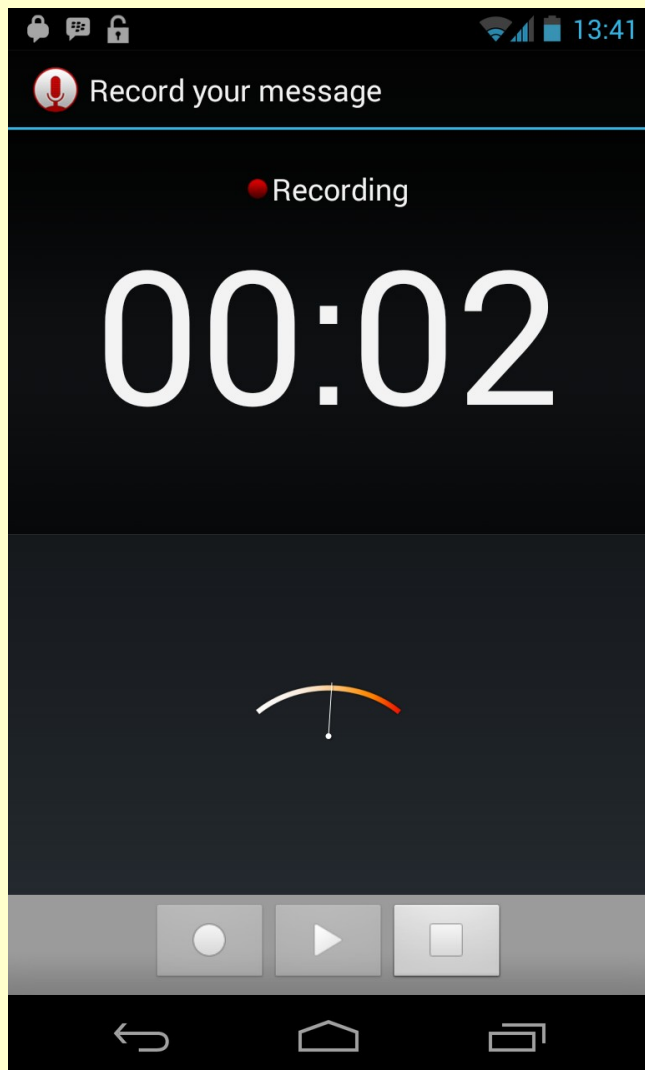
Shema omrežja Tor



...zvočnih komunikacij na mobilnih telefonih



Zvočne komunikacije na mobilnih telefonih preko Tor omrežja



Pogled v (bližnjo) prihodnost...

- Trg pametnih telefonov se povečuje.
- Mobilna omrežja postajajo čedalje bolj zmogljiva.
- Mobilne naprave so čedalje bolj cenovno dostopne.
- VSE komunikacije se selijo na internet.
- Odprtokodne aplikacije za šifriranje komunikacij so brezplačne, interoperabilne in tečejo na različnih operacijskih sistemih.
- 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.”*

**Kaj razvoj tehnologije pomeni za preiskovanje
kaznivih dejanj in kazensko pravo?**

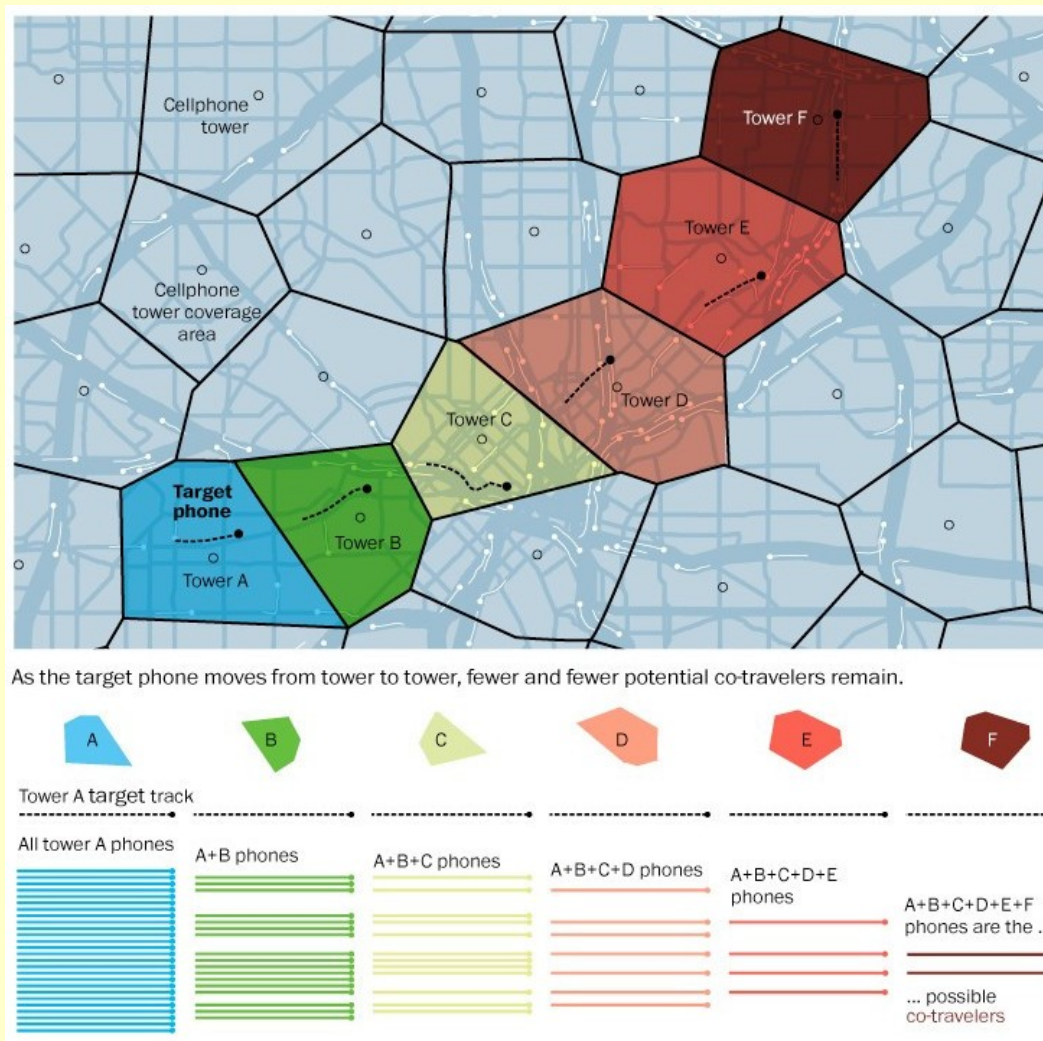
Smo sedaj varni...?

Lokacijska zasebnost

- *“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

Lokacijska zasebnost



Vir in avtorstvo: 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/>

Lokacijska zasebnost

- 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... :-（

Koliko procesorjev ima vaš mobilni telefon?

- Poleg običajnega še procesor na SIM kartici ter na radijskem vmesniku...
- Napadi na radijski vmesnik mobilnega telefona (tim. *baseband processor*, ki je v telefonu **primarni** in na katerem teče *real-time OS*):
 - AT+S0=n: Hayes ukaz za vklop samodejnega odgovora, s katerim je mogoče vključiti mikrofona na mobilniku, izvesti pa ga je mogoče neopazno;
 - uničenje telefona,...
 - več: Ralf-Philipp Weinmann, University of Luxembourg: *The Baseband Apocalypse*.

BUSTED!



Vprašanja?

<http://pravokator.si>

