

Kako zasebno
komunicirati
s pametnimi
telefoni?

Matej Kovačič
<https://pravokator.si>

Nekaj težav
z obstoječo
tehnologijo...

Problem avtentikacije

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

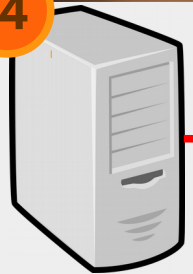
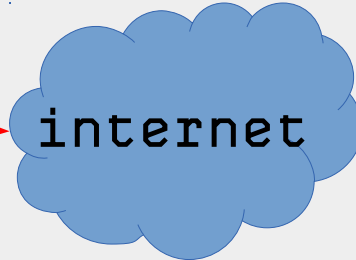
Name/Username	Host	Mask	Port	Status
0 iax2 peers [0 online, 0 offline, 0 unmonitored]				

```
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 ~# _
```

Using account TrixBox local (SIP)

1 2 3
4 abc 5 jkl 6 mno
7 p q r s 8 t u v 9 w x y z
* 0 #



VPN

4

2

3

1

Problem avtentikacije



Problem avtentikacije

	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

Problem prestrezanja

The image displays a network analysis session with several overlapping windows:

- Wireshark (sip.pcap):** Shows a list of captured packets. A filter is applied. The packet list table is as follows:

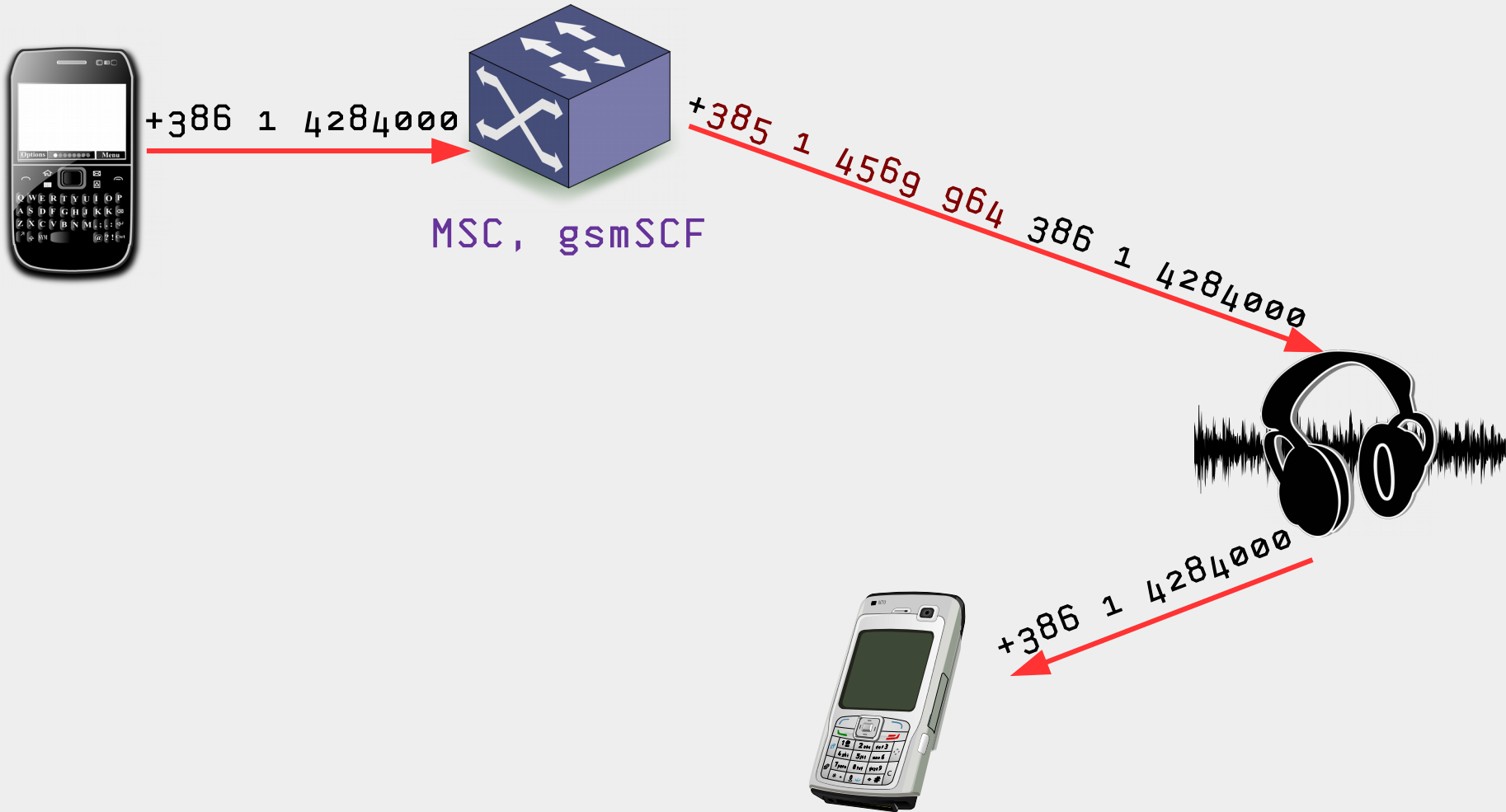
No.	Time	Source	Destination	Length	Protocol	Info
1	20:10:32.318				VoIP Calls	
2	20:10:32.318					
3	20:10:32.667					
4	20:10:32.669					
5	20:10:33.454					
6	20:10:33.454					
7	20:10:39.671					
8	20:10:40.173					
9	20:10:41.175					
10	20:10:42.669					
11	20:10:42.671					
12	20:10:43.179					
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					
- VoIP Calls Summary:** A window titled "Detected 2 VoIP Calls. Selected 1 Call." with a table:

Start Time	Stop Time	Initial Speaker	From	To	Protoco	Packets	State	Comments
21,162982	88,346119		<sip:031		SIP	7	COMPLETE	
102,384695	160,364970	172.16.0.116	"Matej Kovaric" <sip:csip:031		SIP	14	COMPLETE	
- pcap - VoIP - RTP Player:** Shows a timeline of RTP packets. A red box highlights a packet with the following details:

From 172.16.0.116:5062 to [redacted] Duration:64,04 Drop by Jitter Buff:0(0,0%) Out of Seq:0(0,0%) Wrong Tim
- encrypted_srtp_audio:** An audio player window showing a waveform. The frequency is set to 44100 Hz. The waveform shows a significant drop in amplitude at the time of the packet drop.
- Packet Details:** A window showing SIP message details, with several lines highlighted in red:
 - Request: INVITE sip:015805373@212.1, with
 - Response: 100 Trying
 - Request: ACK sip:015805373@212.1
 - Response: INVITE sip:015805373@212.1 with
 - Response: 100 Trying
 - Response: 180 Ringing
 - Response: CANCEL sip:015805373@212.1
 - Response: 200 OK
 - Response: 487 Request Cancelled
 - Response: ACK sip:015805373@212.1

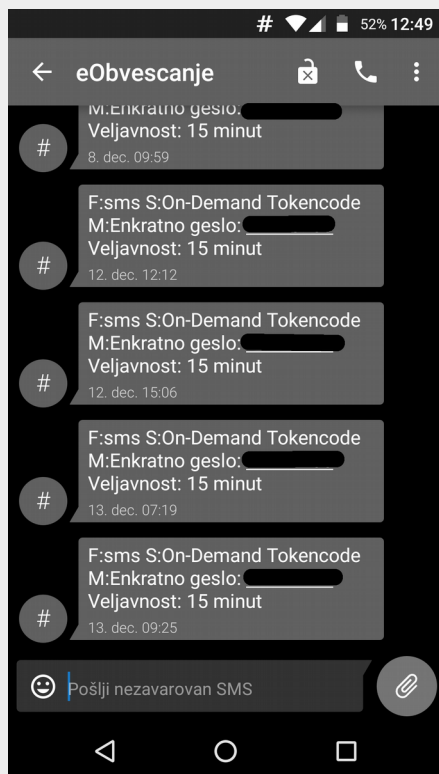
Problem preusmerjanja

...



Problem preusmerjanja

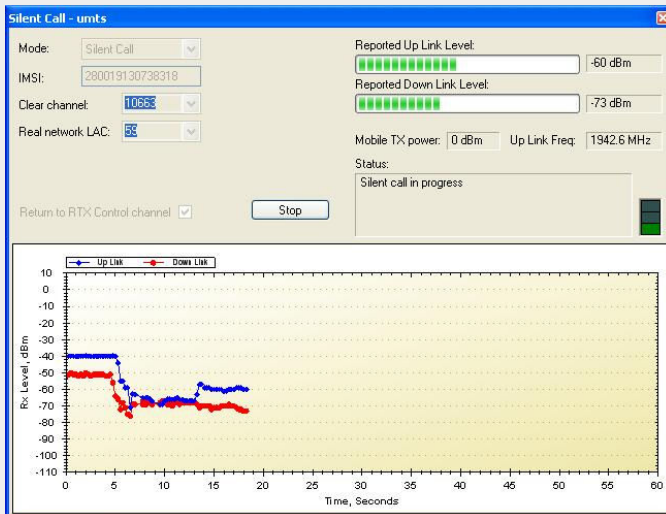
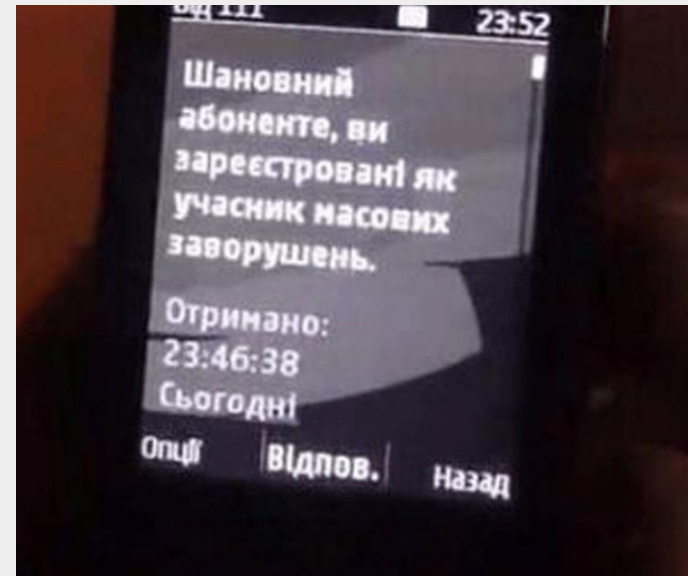
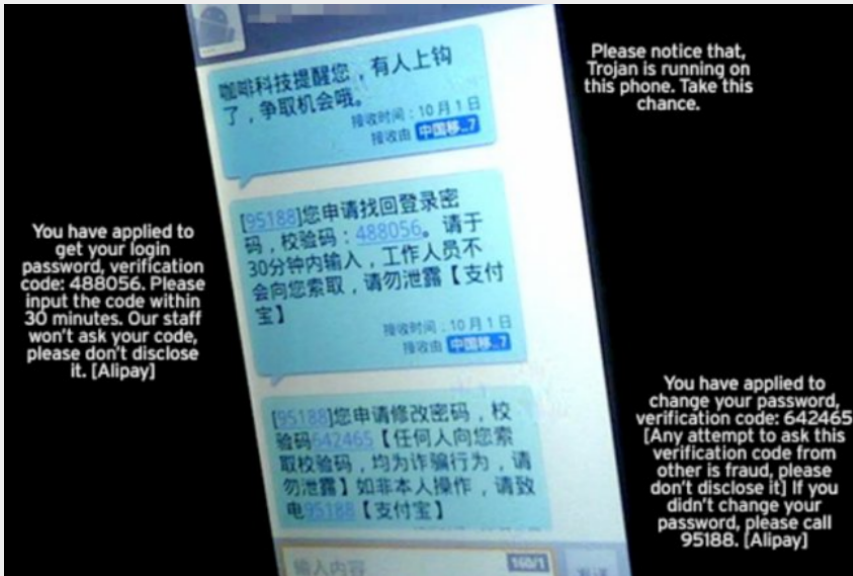
Napadalec se pretvarja, da uporabnik gostuje v njegovem omrežju. S tem doseže, da so dohodni klici in SMS sporočila preusmerjeni k napadalcu.



Zdaj se napadalec prijavi v žrtvino spletno banko in ker žrtev uporablja 2FA, banka po SMS-u pošlje mTAN dostopno kodo...

Ali pa se napadalec skuša prijaviti v službeno omrežje... :-)

Lovilci IMSI številka



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----- X

IN THE MATTER OF AN APPLICATION FOR :
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 280 DRAKE AVENUE, NEW

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

Lovilci IMSI številk

The image shows a Wireshark packet capture window for the interface 'e212.imsi'. The packet list pane shows two packets of type GSM TAP, both with a length of 81 bytes and containing a Paging Request Type 1 message. The packet details pane for the selected packet shows the following structure:

- 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

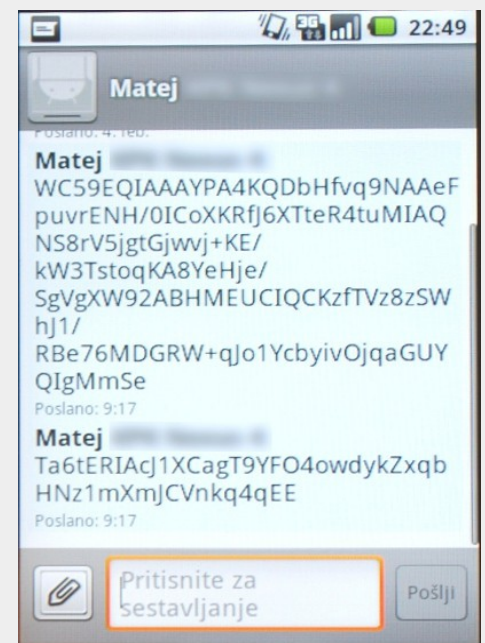
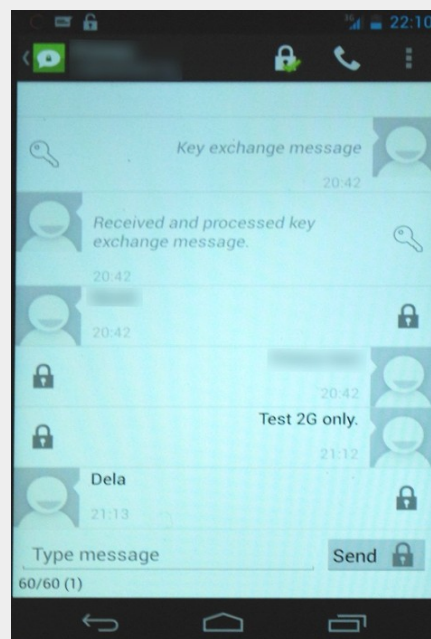
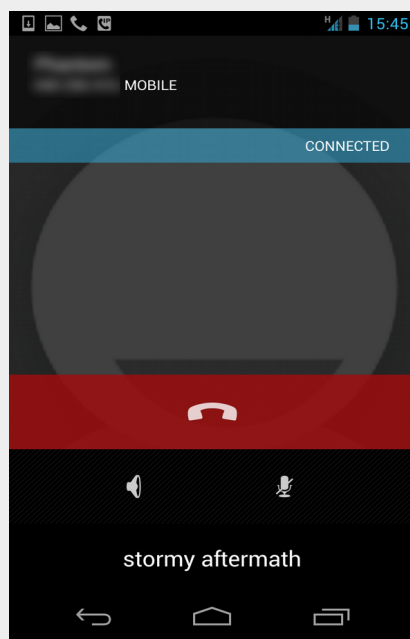
The packet bytes pane shows the raw data for the selected packet:

```
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 +
```

At the bottom of the window, the status bar indicates: International mobile subscriber identity(IMSI) (e212.imsi), 8 bytes | Packets: 4196 · Displayed: 2 (0.0%) · Load time: 0:0.83 · Profile: Default

In nekaj rešitev.

Šifriranje, šifriranje, šifriranje



Prenos podatkov ter šifriranje na aplikacijskem nivoju!

Prometni podatki, anonimizacija

Attachment A

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

Zaobid cenzure, anonimizacija?

Šifriranje "priporočča" tudi NSA

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

Capabilities Development Risk Matrix (II)

	TRIVIAL	MINOR	MODERATE	MAJOR	CATASTROPHIC
Impact > to production Use Risk ↓	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)

Vprašanja?

<https://pravokator.si>