

**Varnost komunikacij
3. del**

Rešitve za zaščito mobilnih komunikacij



**Matej Kovačič
(CC) 2013**

**Kiberpipa – predavanja na temo varnosti mobilne telefonije | Ljubljana, 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 Gorazd Žagar (osebni arhiv) ter navedeni avtorji (C).

Kriptografija

- Beseda kriptografija izvira iz grškega izraza *kryptos logos*, ki pomeni skrita beseda, prvi pa jo je v angleščini uporabil sir Thomas Browne leta 1658.
- Kriptologija je veda o tajnosti, šifriranju, zakrivanju vsebine sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza).
- S pomočjo kriptografije lahko onemogočimo prisluškovanje komunikacijam.
- Kriptoanaliza se ukvarja z razbijanjem šifriranih sporočil.

Nešifriran prenos gesla

921	145.190913	193. [REDACTED]	91. [REDACTED]	TCP	43389 > smtp [ACK] Seq=78 Ack=219 Win=6432 Len=0
922	145.196186	193. [REDACTED]	91. [REDACTED]	SMTP	Command: MAIL FROM:<matej.kovacic@[REDACTED]> SIZE=411
923	145.197425	91. [REDACTED]	193. [REDACTED]	SMTP	Response: 250 OK
924	145.197644	193. [REDACTED]	91. [REDACTED]	SMTP	Command: RCPT TO:<matej.kovacic@[REDACTED]>
925	145.228297	91. [REDACTED]	193. [REDACTED]	SMTP	Response: 250 Accepted
926	145.228621	193. [REDACTED]	91. [REDACTED]	SMTP	Command: DATA
927	145.229646	91. [REDACTED]	193. [REDACTED]	SMTP	Response: 354 Enter message, ending with "." on a line
928	145.236472	193. [REDACTED]	91. [REDACTED]	SMTP	DATA fragment, 414 bytes
929	145.243559	91. [REDACTED]	193. [REDACTED]	SMTP	Response: 250 OK id=1KMGLN-0001x3-7M
930	145.246496	193. [REDACTED]	91. [REDACTED]	SMTP	DATA fragment, 6 bytes
931	145.247380	91. [REDACTED]	193. [REDACTED]	SMTP	Response: 221 [REDACTED] closing connection
932	145.247621	91. [REDACTED]	193. [REDACTED]	TCP	smtp > 43389 [FIN, ACK] Seq=396 Ack=583 Win=6432 Len=0
933	145.287572	193. [REDACTED]	91. [REDACTED]	TCP	43389 > smtp [ACK] Seq=583 Ack=397 Win=6432 Len=0
934	145.403764	193. [REDACTED]	91. [REDACTED]	TCP	43389 > smtp [FIN, ACK] Seq=583 Ack=397 Win=6432 Len=0
935	145.404693	91. [REDACTED]	193. [REDACTED]	TCP	smtp > 43389 [ACK] Seq=397 Ack=584 Win=6432 Len=0

Frame 919 (111 bytes on wire, 111 bytes captured)

Ethernet II, Src: [REDACTED] ([REDACTED]), Dst: [REDACTED] ([REDACTED])

Internet Protocol, Src: 193. [REDACTED] (193. [REDACTED]), Dst: 91. [REDACTED] (91. [REDACTED])

Transmission Control Protocol, Src Port: 43389 (43389), Dst Port: smtp (25), Seq: 21, Ack: 219, Len: 57

SMTP, Seq: 21, Len: 57

Command: AUTH PLAIN AG1hdGVqLmtvdmFjaWNAKioqKiouc2kAZ2VzbG8hrg==\r\n

Command: AUTH PLAIN AG1hdGVqLmtvdmFjaWNAKioqKiouc2kAZ2VzbG8hrg==

Uporabniško ime in geslo sta Base64 kodirana...

Command: AUTH PLAIN matej.kovacic@*****.si | geslo!

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

- *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

Sodobna kriptografija

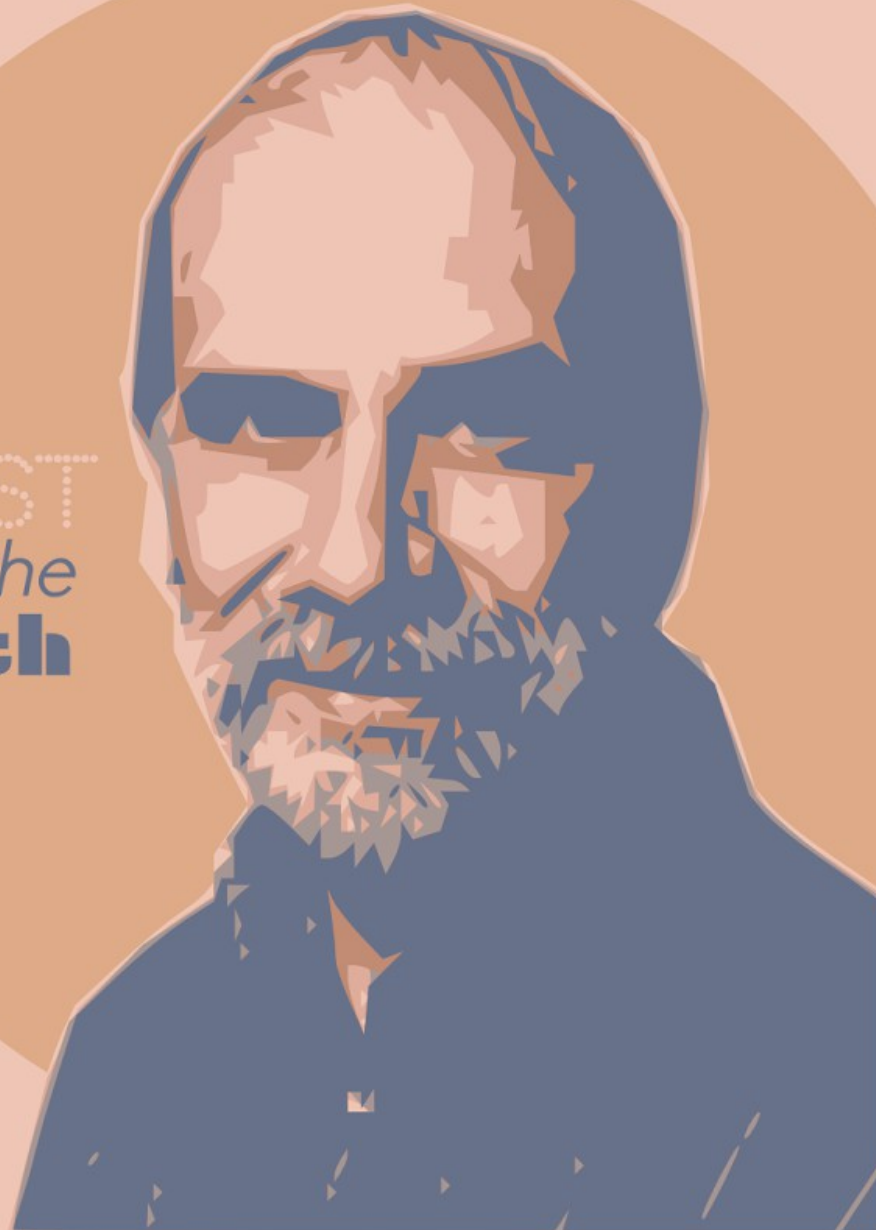
- *»Varnost šifrirnih sistemov naj temelji na računski zapletenosti.«*

-- John Forbes Nash v pismu NSA leta 1955
(ta ideja je v kriptografiji prevladala šele 20 let kasneje)

- *»We have to make surveillance expensive again.«*

-- Bruce Schneier, 2013

TRUST
the
math



Točke zloma sodobnih šifrirnih sistemov

- **Varnost terminalnih naprav** (tim. *endpoint security*) – prestrezniki tipkanja, zlonamerna programska oprema,...
- Zaupanje izdajateljem digitalnih potrdil (*Certificate Authorities*).
- Skrite funkcionalnosti v šifirnih čipov (tim. *crypto accelerator hardware*) - uhajanje šifrirnih ključev preko porabe električne energije ali s časovnimi napadi, kleptografski napadi na generiranje šifrirnih ključev,...
- Napadi na šifrirne algoritme in generatorje naključnih števil (Dual EC DRBG, Intelov strojni RDRAND, RC4, špekulacije o napadih na eliptične krivulje,...).
- **Prometni podatki.**

Varnost terminalnih naprav

- *»On the Internet, communications security is much less important than the security of the endpoints. And increasingly, we can't rely on cryptography to solve our security problems..«*

-- Bruce Schneier

Zasnova sodobnih aplikacij za varno komuniciranje

- Šifriranje komunikacij med končnima točkama, skupaj s sistemom za overjanje komunikacijskih partnerjev.
- Uporaba poudarjene zaupnosti (ang. *perfect forward secrecy*).
- Šifriranje prometnih podatkov/signalizacije.
- Šifriranje podatkov v lokalni shrambi.

Zasnova sodobnih aplikacij za varno komuniciranje

- Podpora za povezovanje preko posredniških sistemov (ang. *proxy*) oziroma anonimizacijskega Tor omrežja.
- »*Panic button*«.

Zasnova sodobnih aplikacij za varno komuniciranje

- »Pripenjanje« digitalnih potrdil (ang. *Certificate Pinning*) - ne upoštevamo CA hierarhije, pač pa preverimo ali je certifikatska »veriga« taka, kot pričakujemo).
- TOFU/POP (*Trust On First Use / Persistence Of Pseudonym*), gre za kontinuiteto šifrirnih ključev oz. možnost ročnega preverjanja digitalnih potrdil.

Rešitve **že** obstajajo

- 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**.

Zakaj?

Notranji napad in sodna odredba

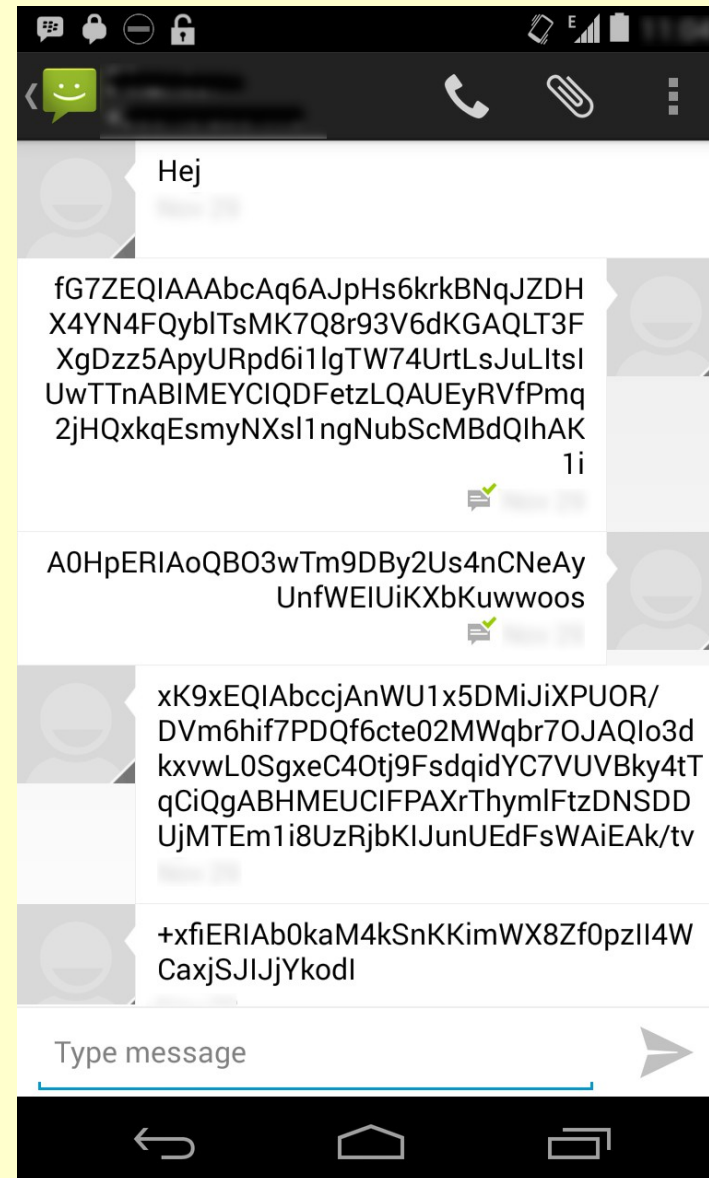
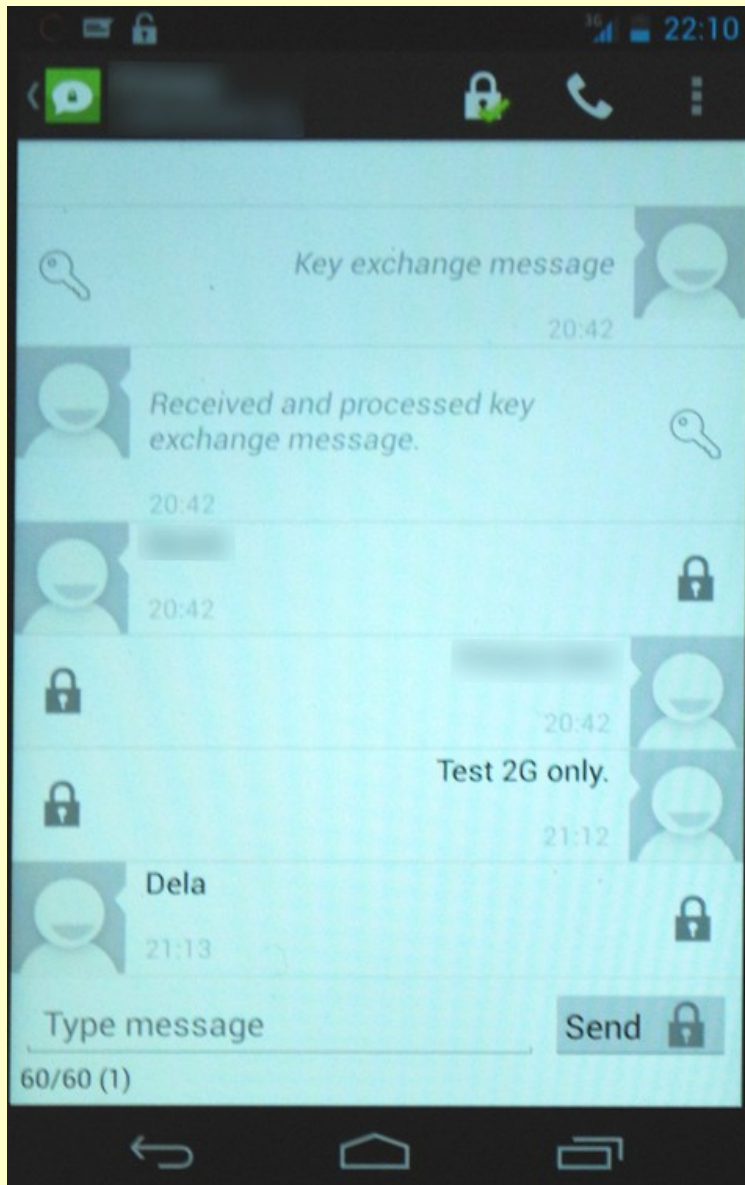
»To see why, consider two companies, which we'll call Lavabit and Guavabit. At Lavabit, an employee, on receiving a court order, copies user data and gives it to an outside party -- in this case, the government. Meanwhile, over at Guavabit, an employee, on receiving a bribe or extortion threat from a drug cartel, copies user data and gives it to an outside party -- in this case, the drug cartel.

From a purely technological standpoint, these two scenarios are exactly the same: an employee copies user data and gives it to an outside party. ... Technical measures that prevent one access scenario will unavoidably prevent the other one.«

-- Ed Felten, 2013, A Court Order Is an Insider Attack

Primeri rešitev.

Šifrirana SMS sporočila: TextSecure




Šifrirana SMS sporočila: TextSecure

CyanogenMod Installer


- 1 Allow installation of the CyanogenMod Installer Application**

Open the **Settings** application and navigate to **Security** (on some devices, you may need to navigate to **Applications**). Locate the **Unknown sources** option.



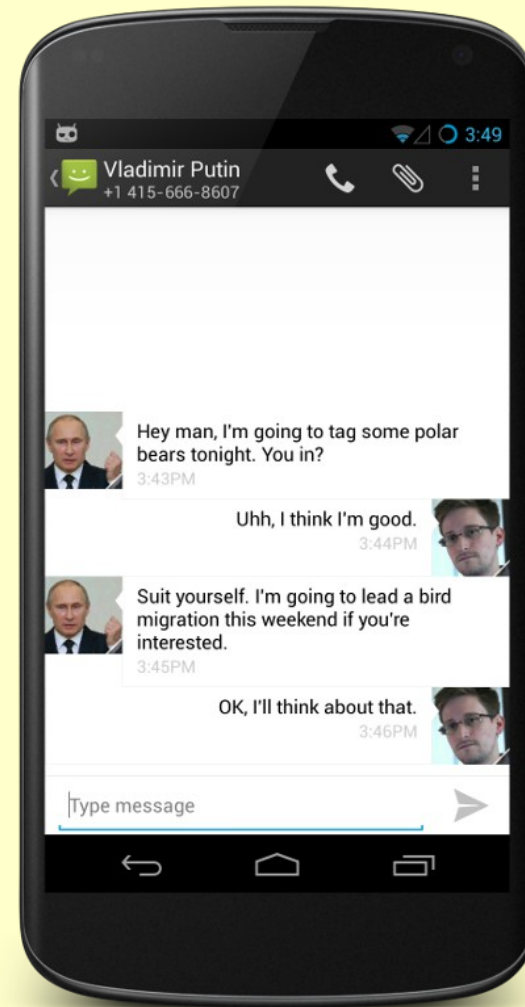
If **Unknown sources** is already checked, you can skip this step.
If unchecked, tap the checkbox and then tap **OK** on the confirmation popup.
- 2 Download the CyanogenMod Installer Application**

From your Android phone or tablet, visit <http://get.cm/app> using your web browser or scan the QR code.


- 3 Install the CyanogenMod Installer Application**

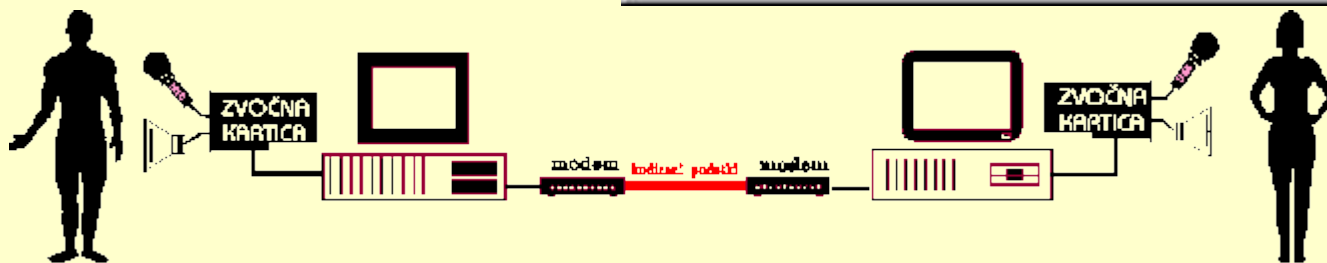
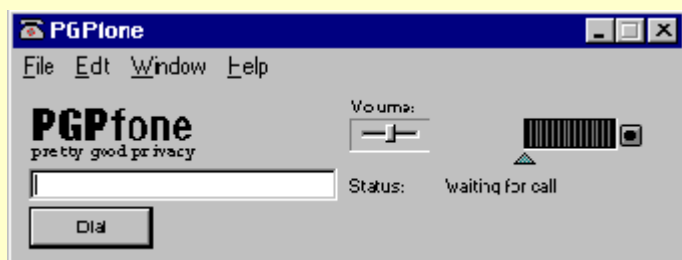
When the download is complete, open your notifications and tap **OneClick.apk**.
Tap **Install**.
Tap **Open**.
Follow the instructions displayed on your Android phone or tablet to continue the installation process.
- 4 Download the CyanogenMod Windows Installer**

[Click here](#) to download the CyanogenMod Installer for Windows Vista/7/8.
Run the CyanogenMod Installer for Windows and follow the on-screen instructions.



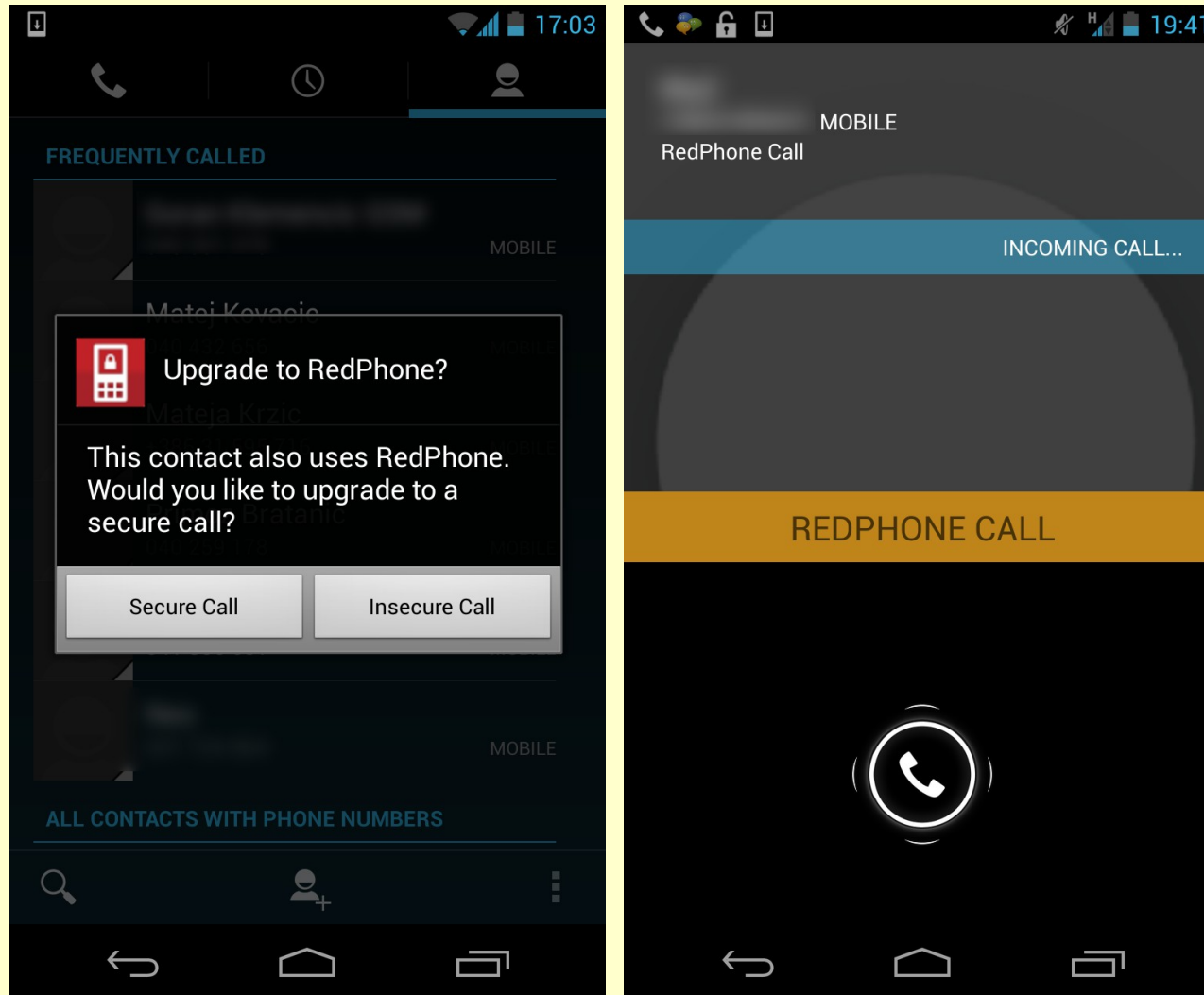
TextSecure prihaja privzeto na CyanogenMod (10 mio. uporabnikov!) ter na iPhone. Avtentikacija uporabnikov, uporaba SMS ali podatkovnega kanala,...

Pogled v zgodovino: PGPfone, 1995



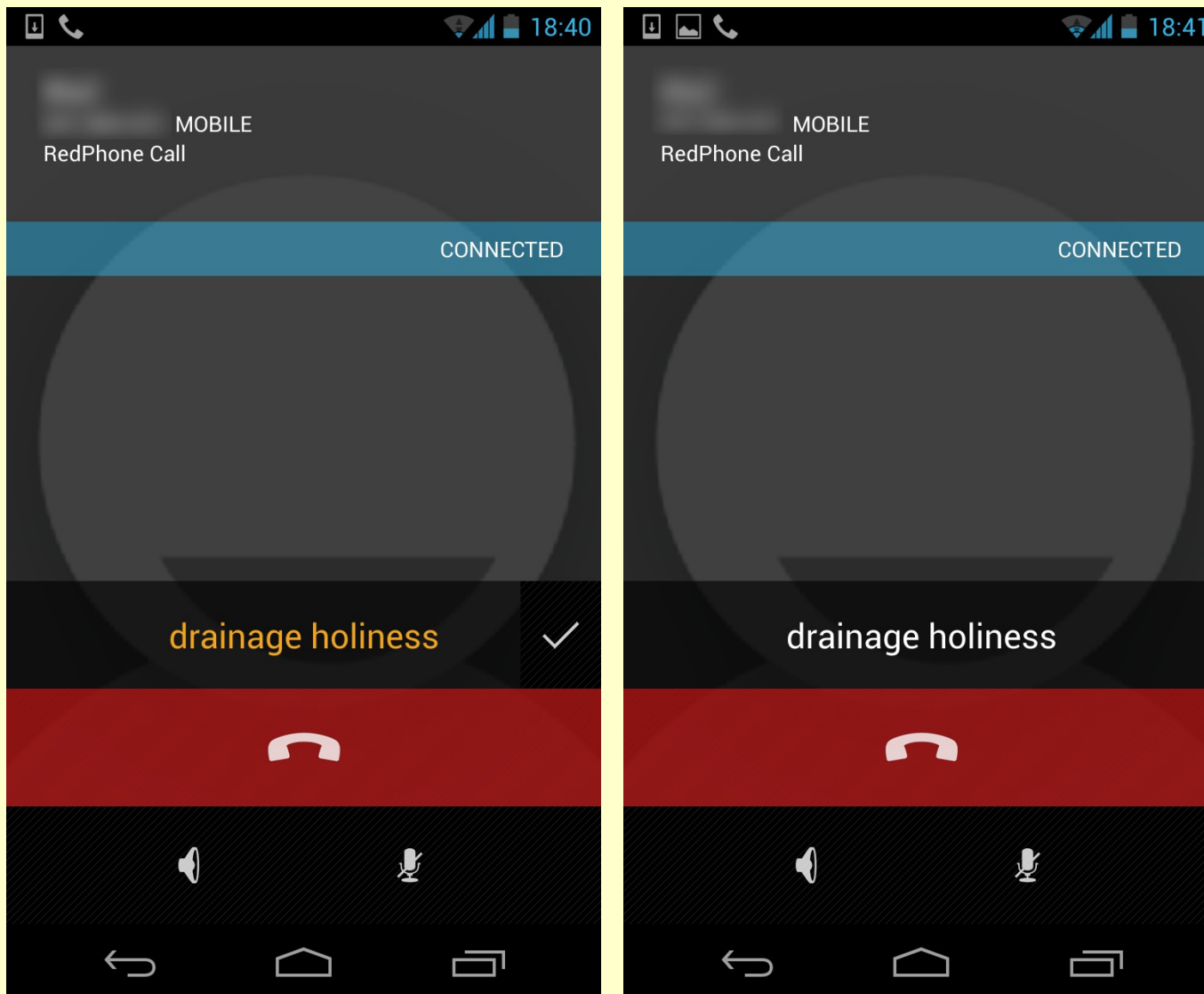
PGPfone je Zimmerman razvil sredi 1990-tih let, omogočal je komunikacijo preko modemov ali interneta, vendar takrat tehnologija še ni bila zrela za splošno uporabo...

Šifrirani telefonski pogovori: RedPhone



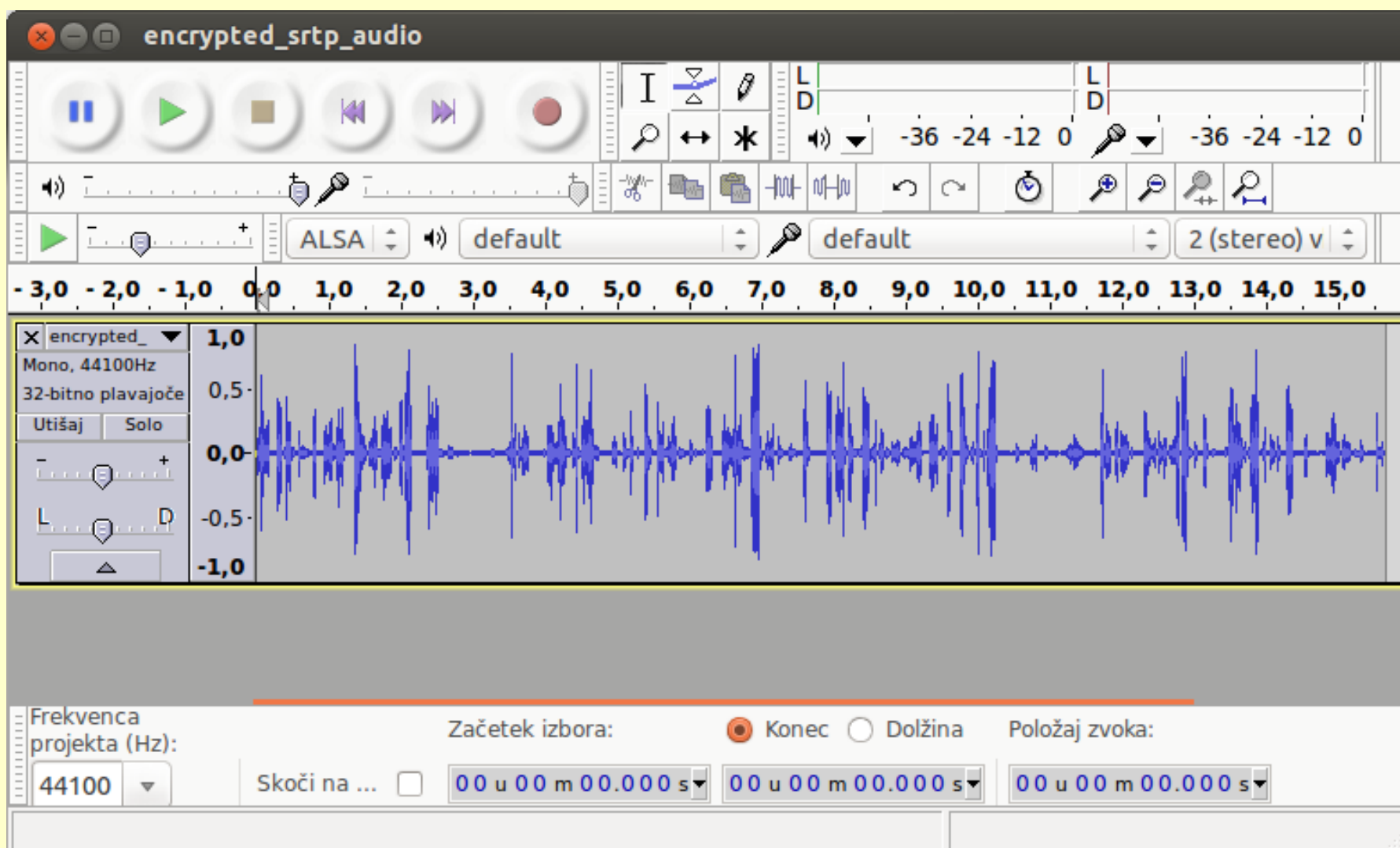
Integracija v sistem, »zapečeni« TLS ključi za šifriranje signalizacijskih metapodatkov, brez VBR in VAD... Problem: identifikator je še vedno telefonska številka.

Šifrirani telefonski pogovori: RedPhone



TOFU/kontinuiteta šifrirnega ključa, PFS... vse to se izvaja v ozadju.

Kako je slišati šifriran telefonski pogovor?

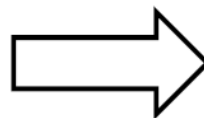


[Demo]

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

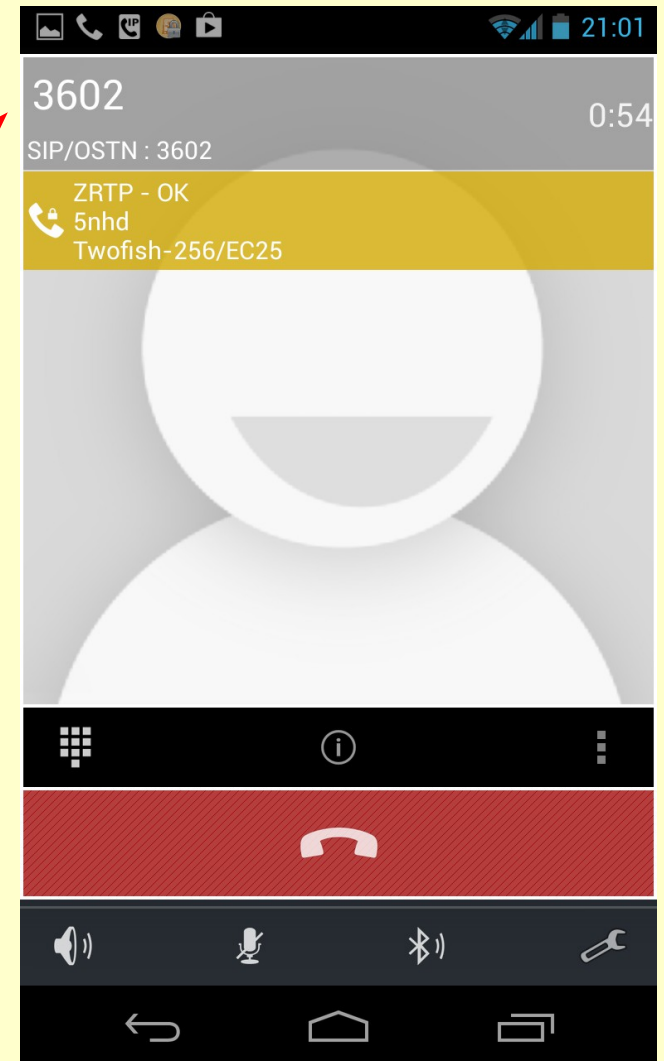
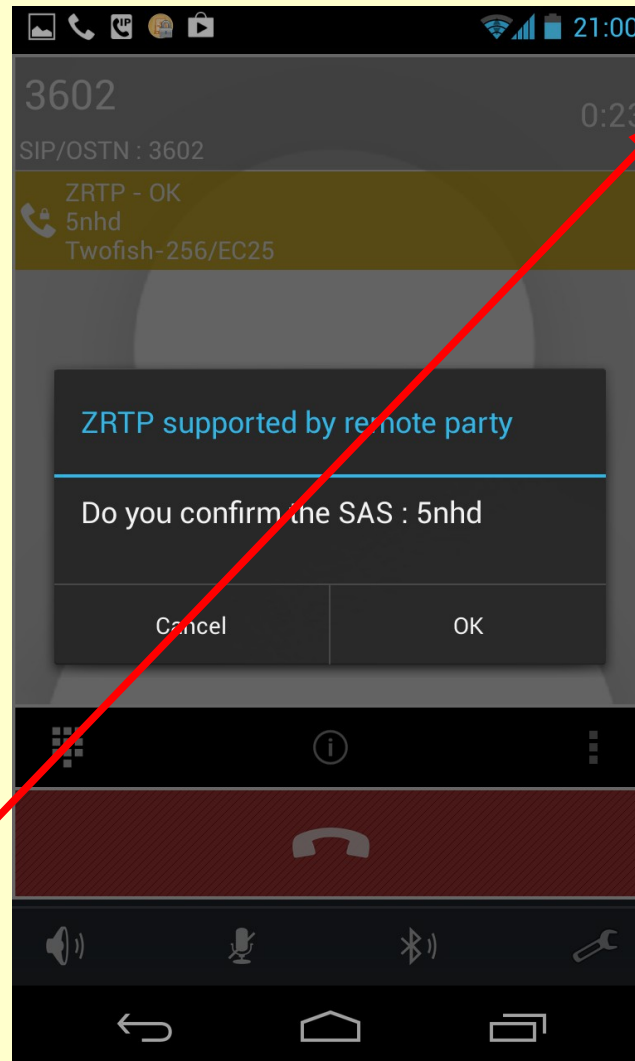
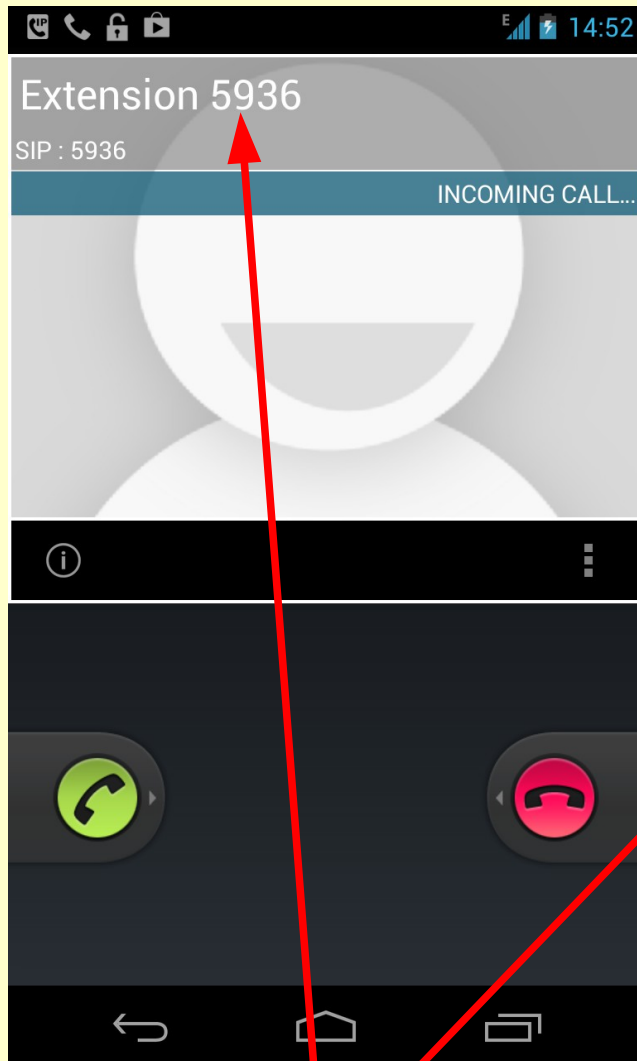


tip klica	klicana oseba	datum in čas	trajanje
RP klic	Nemčija	Jun 1, 2013 12:52:36 PM	37
RP klic	Nemčija	Jun 1, 2013 12:53:28 PM	23
RP klic	Nemčija	Jun 1, 2013 12:54:40 PM	22
RP klic	Nemčija	Jun 1, 2013 12:59:26 PM	17

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

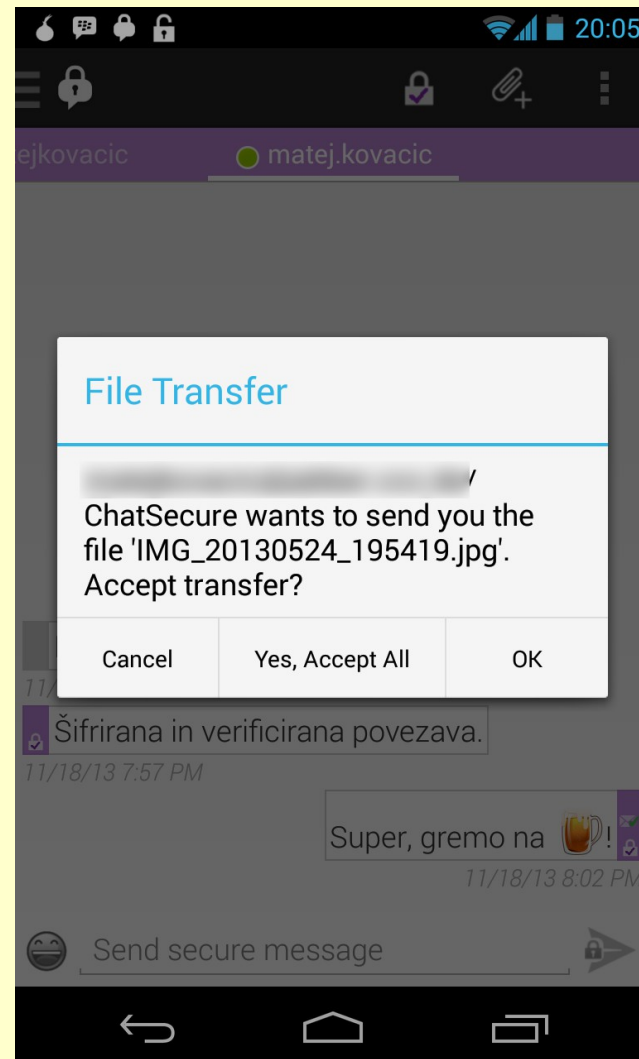
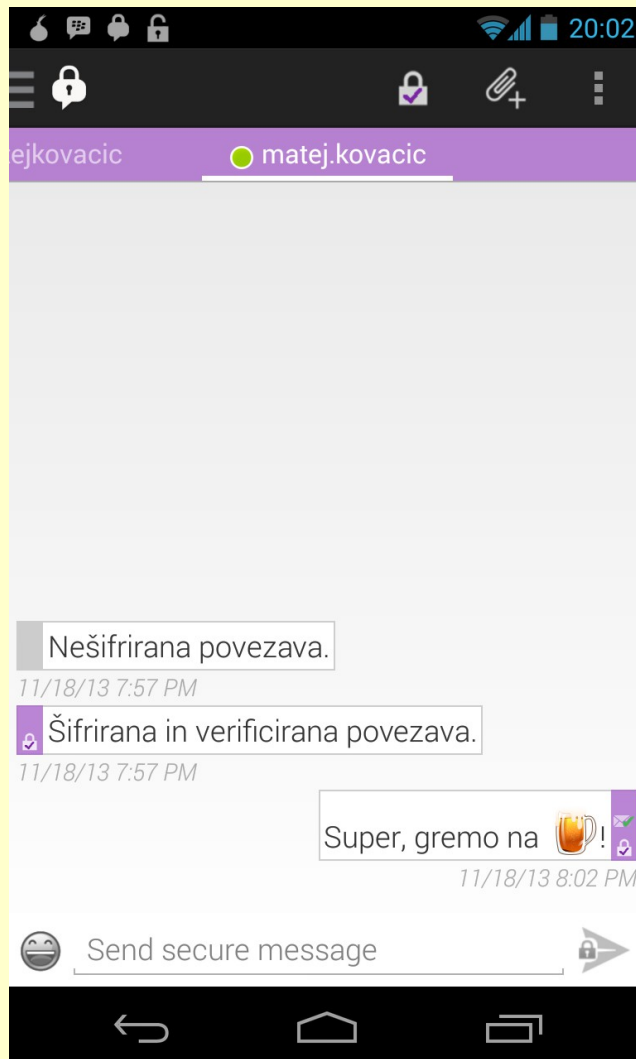
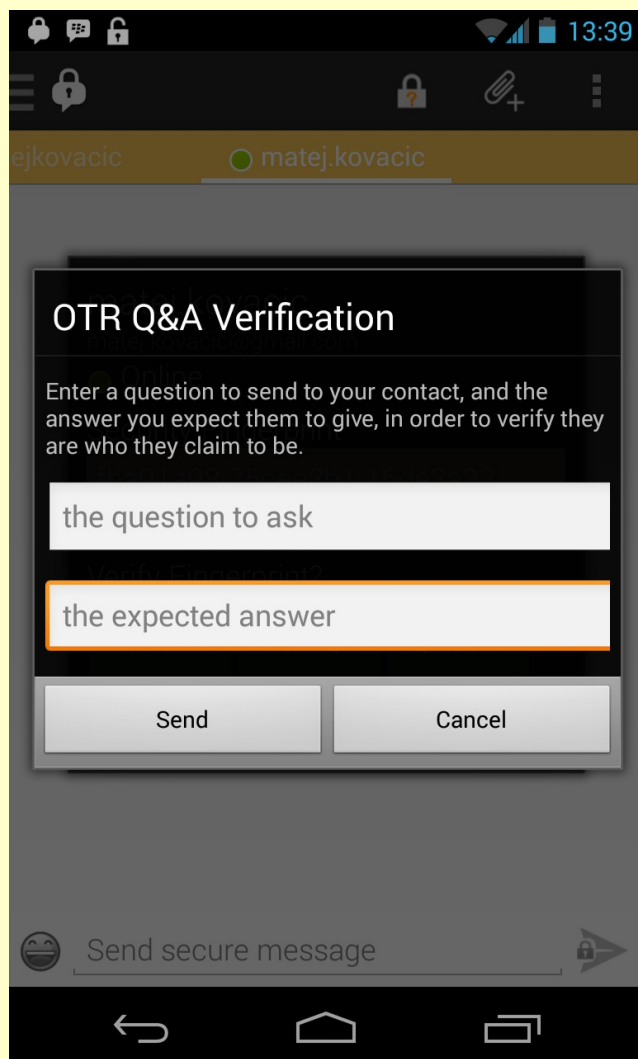
tip klica	klicana oseba	datum in čas	trajanje
RP klic	Slovenija3	Jun 2, 2013 10:47:14 AM	11
RP klic	Slovenija3	Jun 2, 2013 10:47:52 AM	64
RP klic	Slovenija3	Jun 2, 2013 10:49:03 AM	102
RP klic	Slovenija3	Jun 2, 2013 10:50:52 AM	70
RP klic	Slovenija4	Jun 2, 2013 11:59:36 AM	2
RP SMS	Slovenija4	Jun 2,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

Šifrirana IP telefonija: CsipSimple ter OSTN



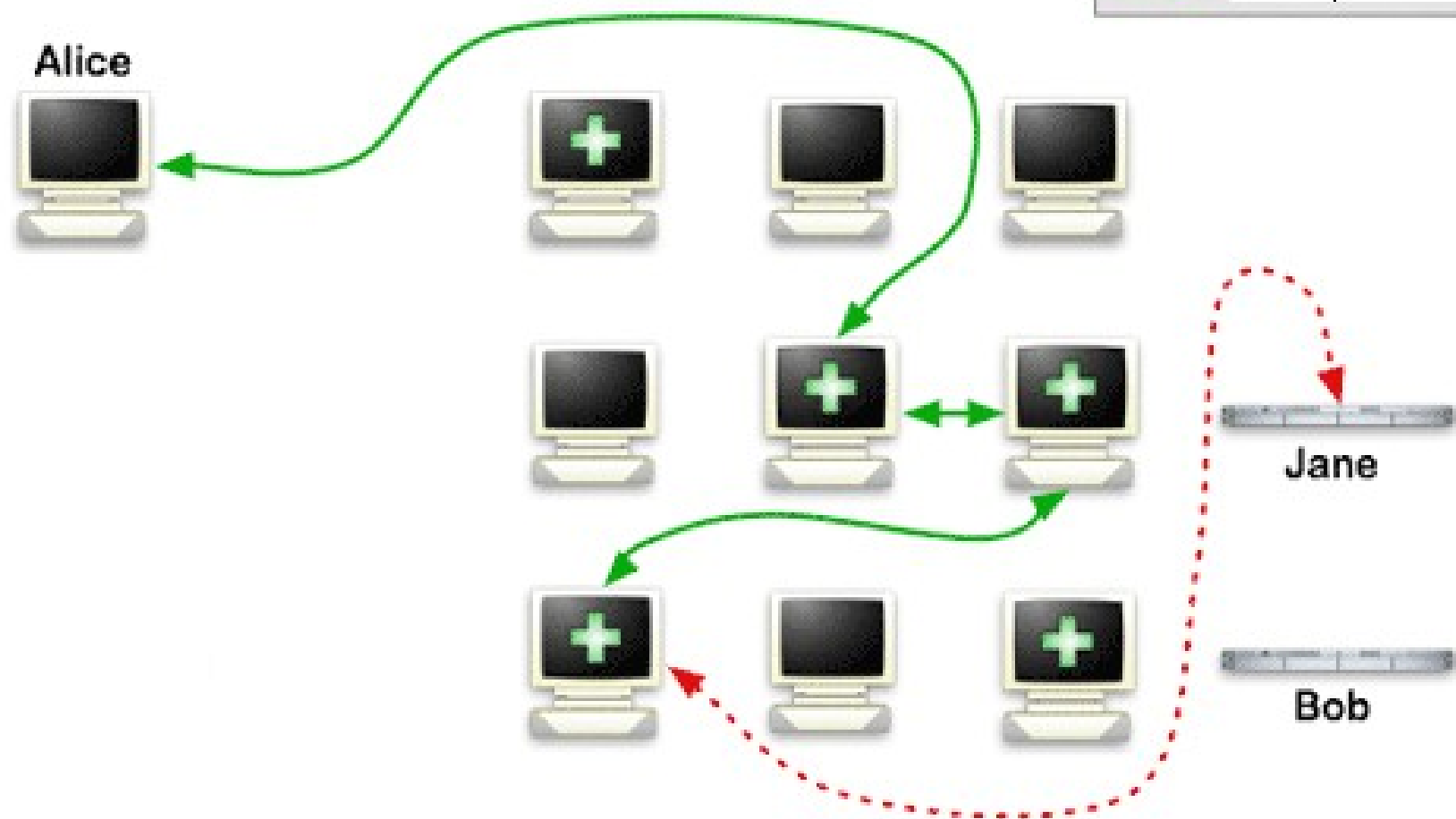
Prometni podatki?

Šifrirana hipna sporočila: ChatSecure in XMPP

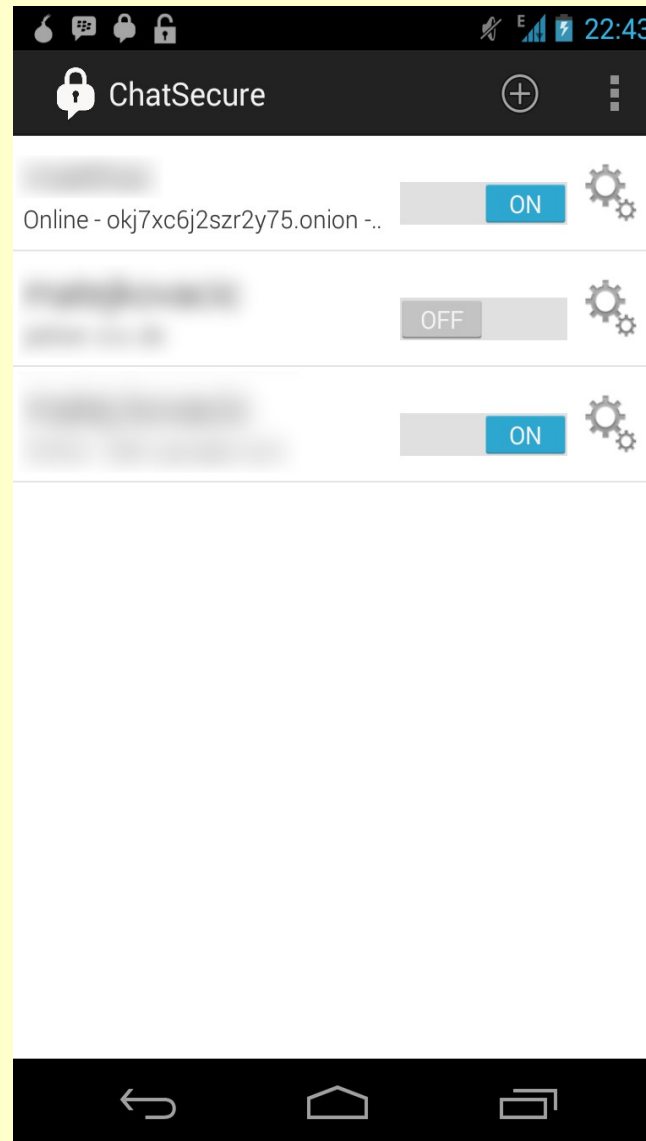
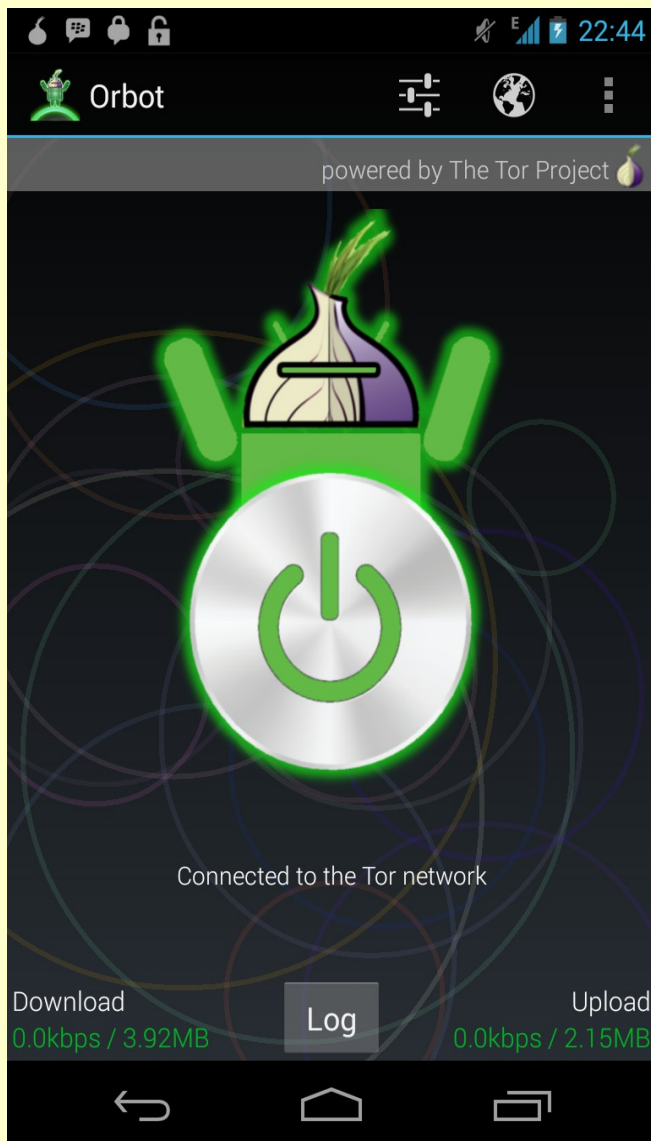


Anonimizacija...

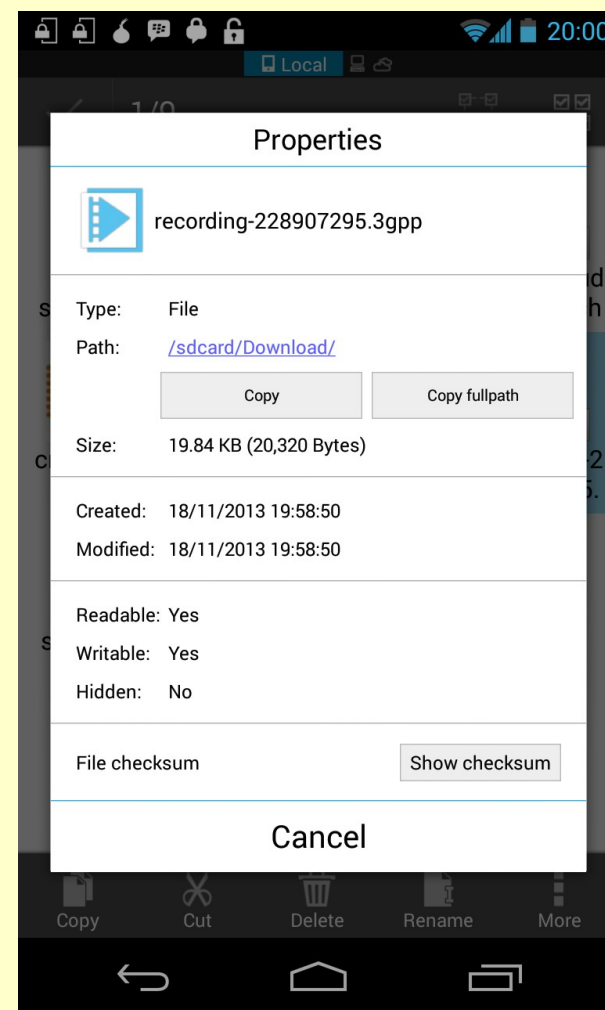
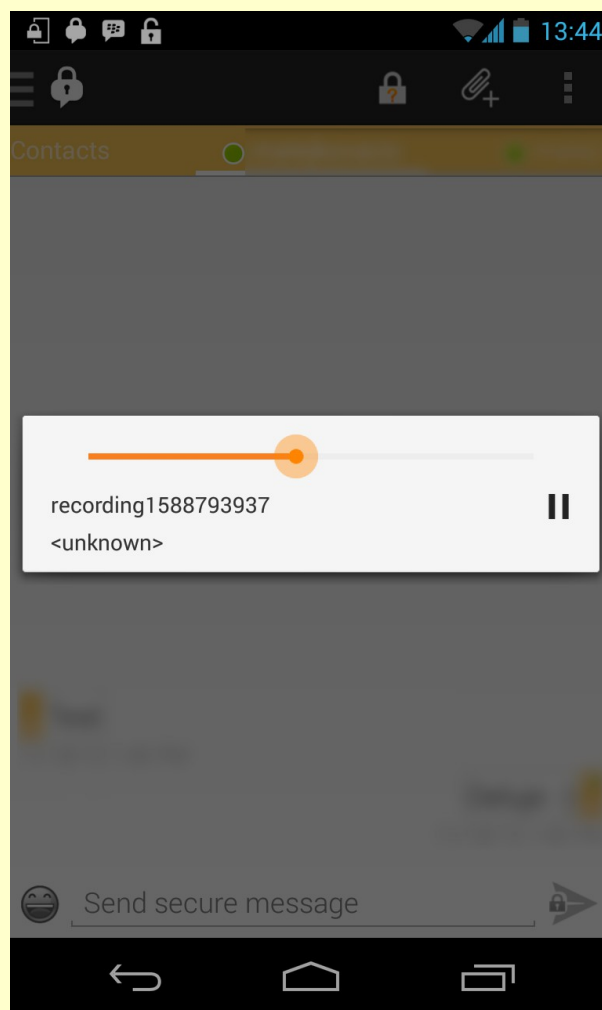
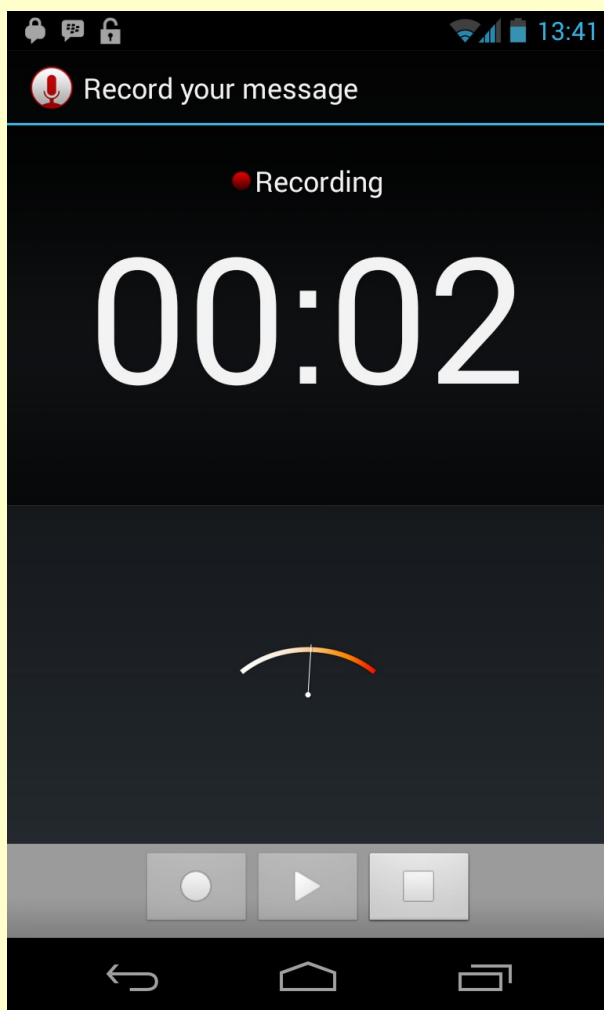
Shema omrežja Tor



...zvočnih komunikacij na mobilnih telefonih

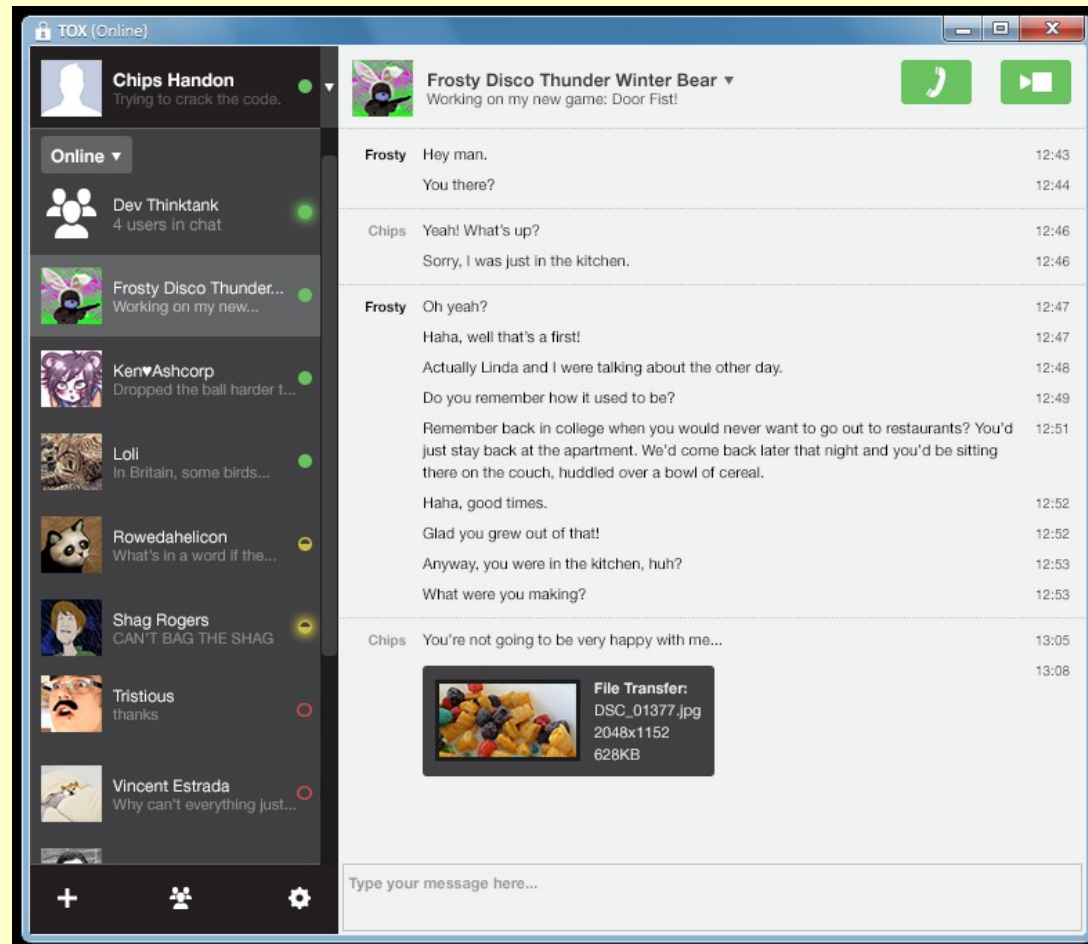


Zvočne komunikacije na mobilnih telefonih preko Tor omrežja



Visoka latenca Tor omrežja, rešitev: komunikacija je asinhrona, zato ni problema trepetanja (ang. *jitter*) ter echo efekta.

Tox



Varna zamenjava za Skype.

P2P, šifrirane komunikacije, brez potrebe po kakršnikoli konfiguraciji.

V razvoju, prva različica bo na voljo za Linux, Windows in Mac sisteme konec leta...

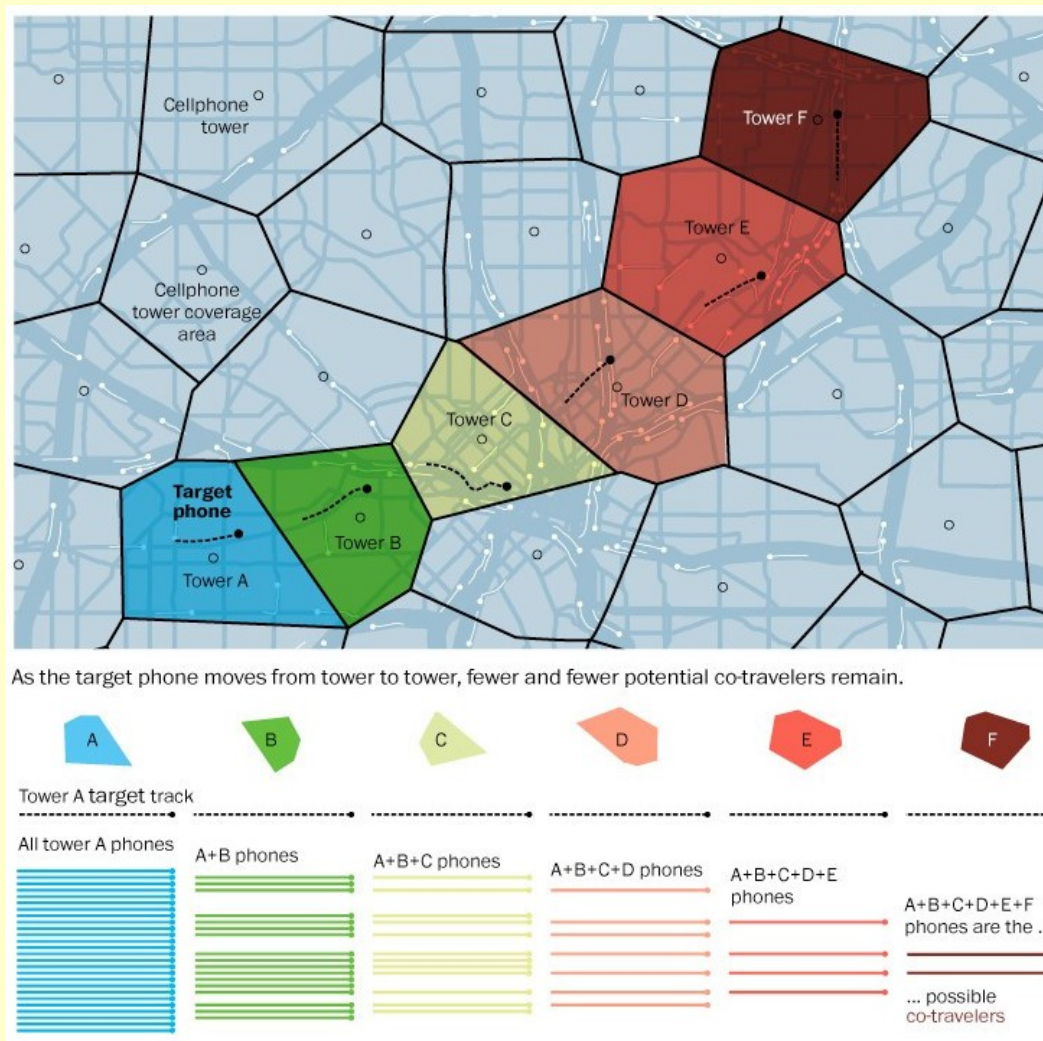
Ampak... smo sedaj *res* varni?

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...
- ... mogoči so tudi napadi na radijski vmesnik mobilnega telefona (tim. *baseband processor*, ki je v telefonu **primarni** in na katerem teče *real-time OS*).

(Vklop mikrofona, blokada ali uničenje telefona, nadzor nad strojno opremo, itd.).

Vendar pa...

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.”*
- Prisluškovanje spet postaja »drago«.



Vprašanja?



Ilustracija: (CC) SulphurSpoo © DeviantArt

<http://pravokator.si>

