VoLTE Phreaking

Haxpo Track, Hack in the Box Conference, 9 May 2019

Secura

© 2018. Proprietary & Confidential.

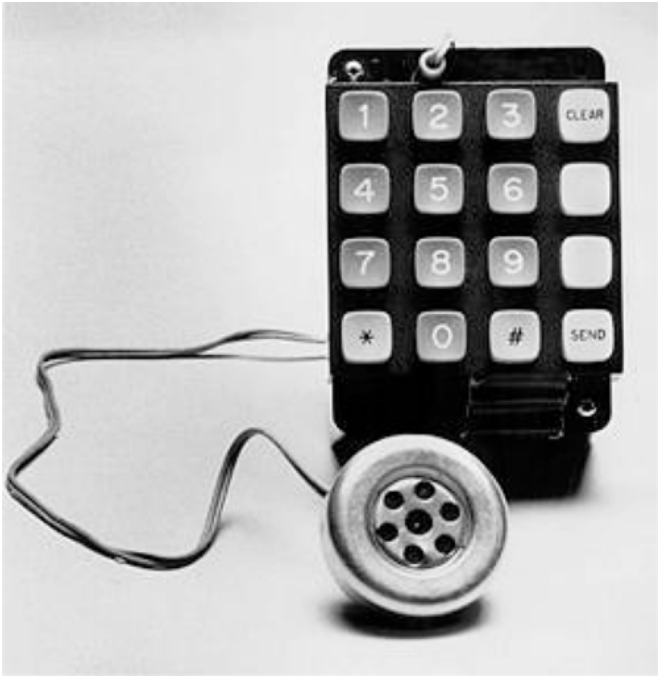
Who am I?

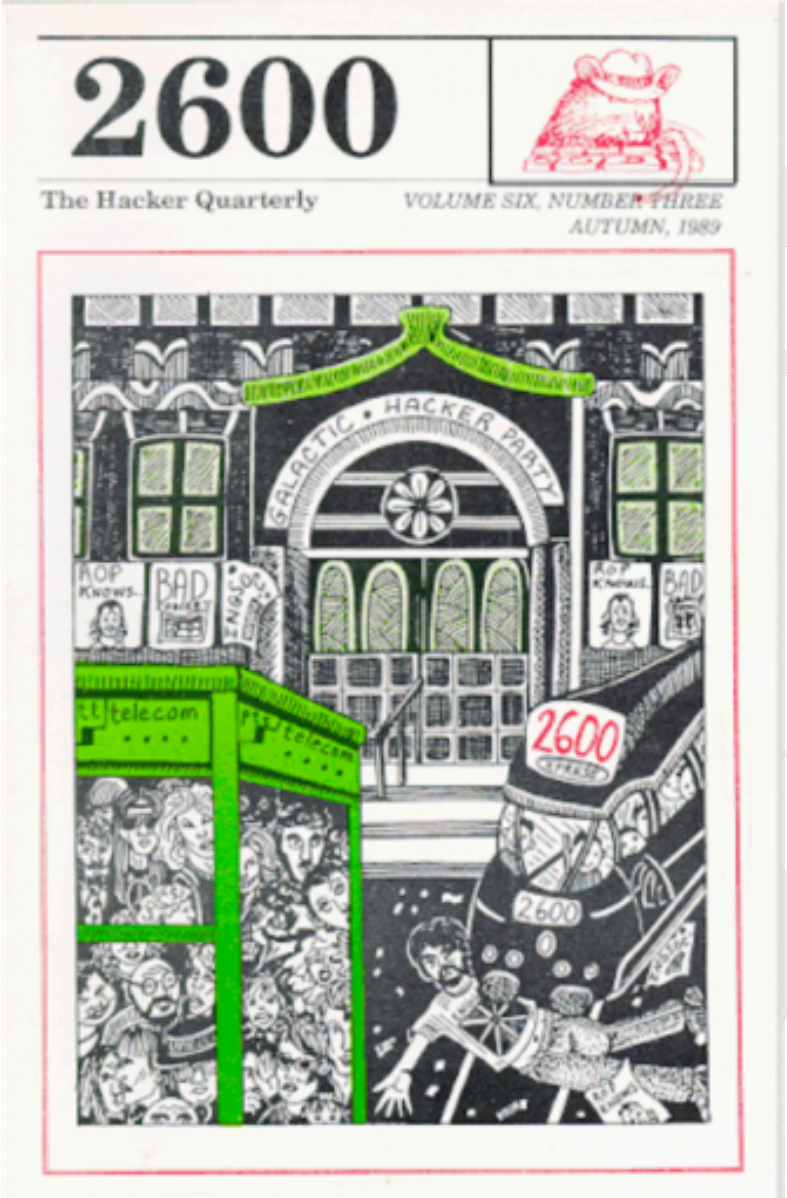
- Ralph Moonen
- Technical Director at Secura
- Old school phreak

Agenda

- A little history of telephony hacking (in NL/EU)
- The landscape now
- Intercepting communications in 2019
- Vulnerabilities discovered: some new, some old
- An app to monitor traffic on a phone

History





Secura

History

- Signalling systems:
  - Like DTMF but with other frequencies
  - Could be heard whilst setting up call
  - Could/can also be injected by end-user (analog phreaking not completely 100% definitively dead yet)
  - Trick exchange into thinking end-user is also exchange
  - R1, R2, CCITT4, CCITT5
  - ftp://ftp.wideweb.com/GroupBell

History in NL

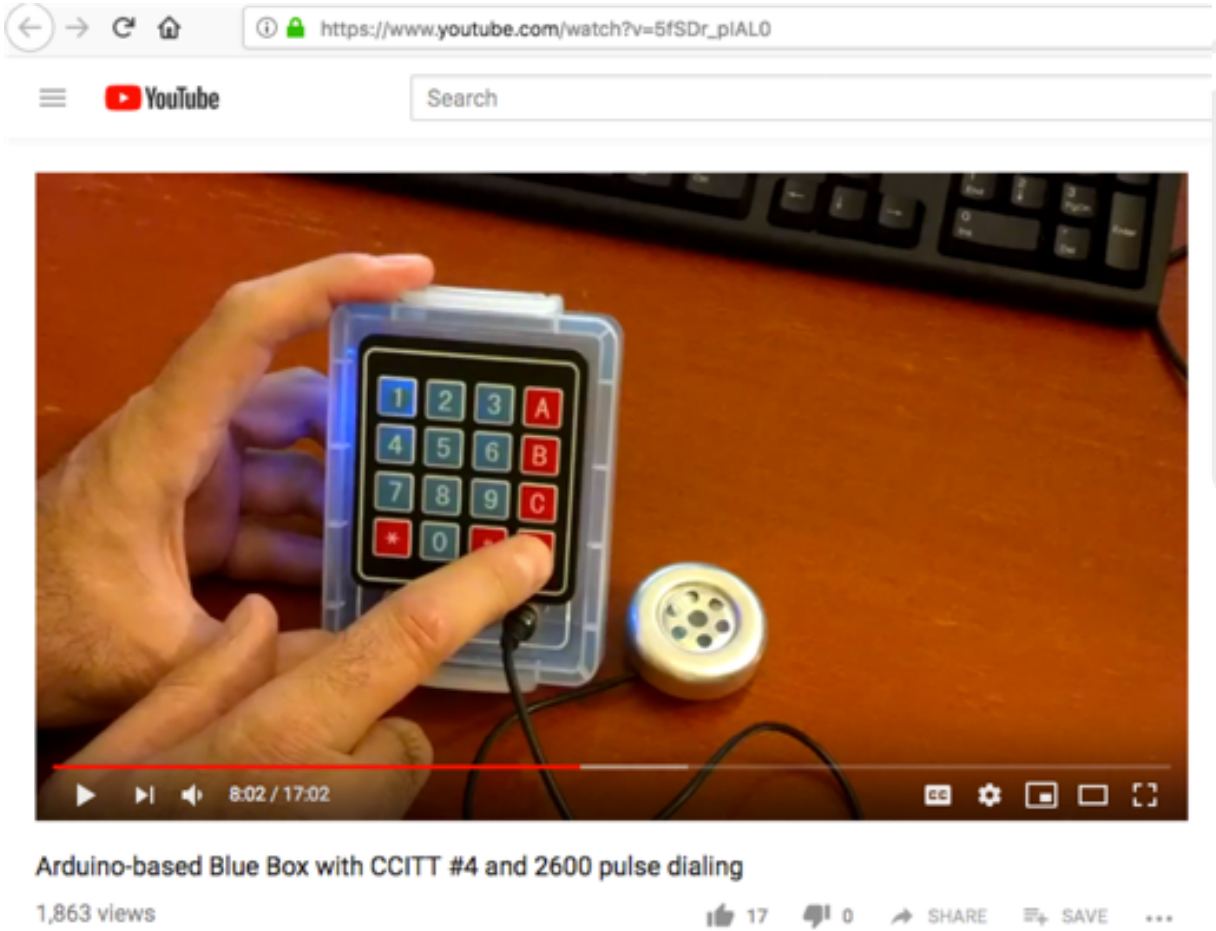
- 80’s: a group in NL found that this also worked in for our phone network.
- Back then, 06-022XXXX were toll-free (now 0800-numbers)
- Often international lines: faxes, hotel reservations, modems, etc.
- Allowed phreaking!

Secura

History in NL

- Blue box, brown box, green box: the rainbow warrior
- Endless phun!
- Make phree phone calls, get connected to chatrooms, secret switchboards, operators in Korea, the White House, CIA, FBI, and lots of modems.
- Remember: dial-in lines were expensive

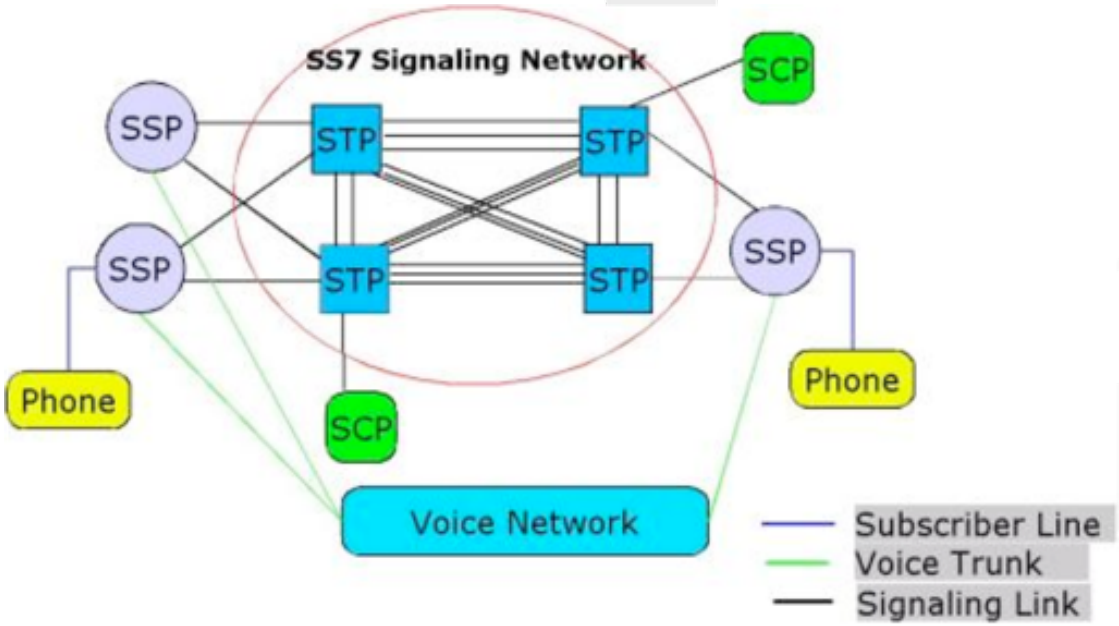
Play around yourself



Secura

Digital

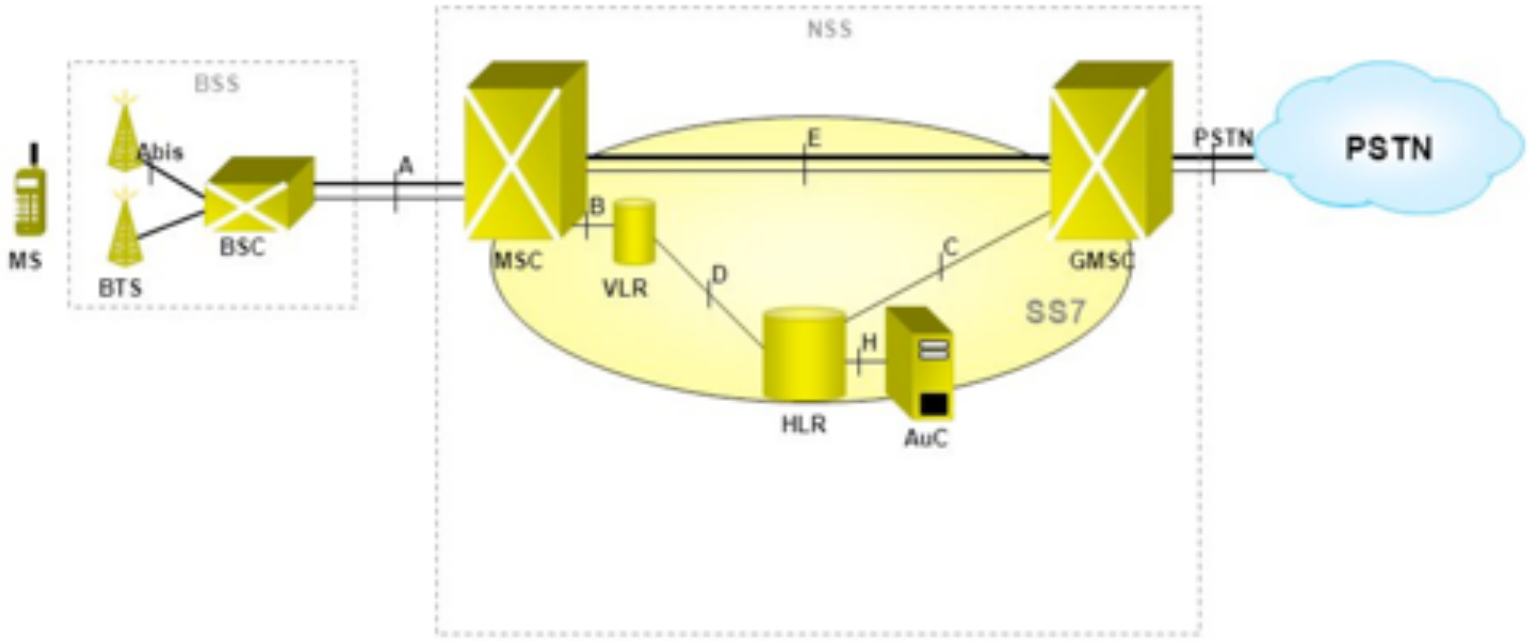
- Late 80’s, early 90’s, we transitioned to ISDN, digital lines
- SS7 was introduced
- Still used and abused
- OOBSS



Secura

Mobile

GSM 2G Architecture



BSS — Base Station System

BTS — Base Transceiver Station

BSC — Base Station Controller

MS — Mobile Station

NSS — Network Sub-System

MSC — Mobile-service Switching Controller

VLR — Visitor Location Register

HLR — Home Location Register

AuC — Authentication Server

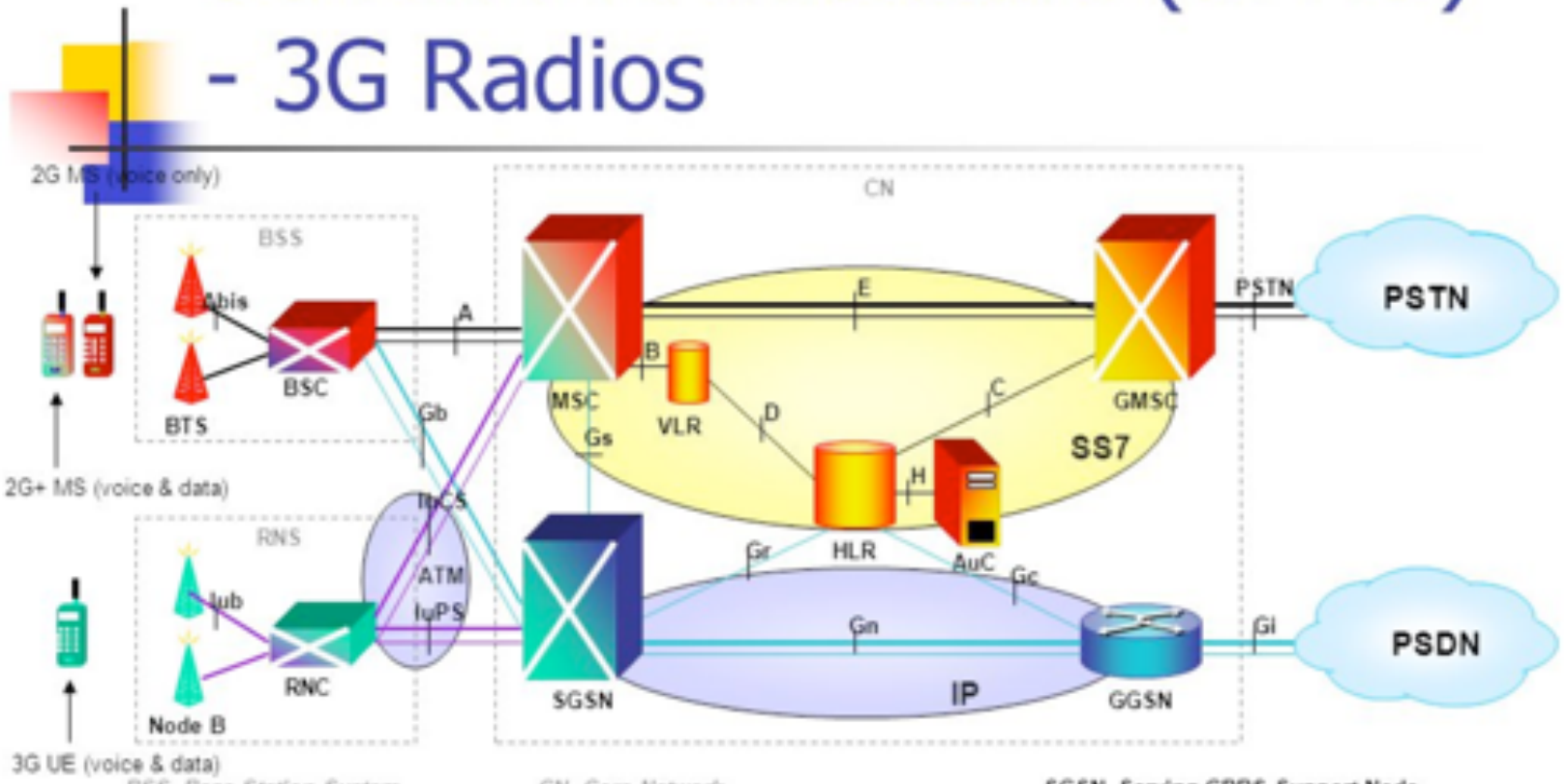
GMSC — Gateway MSC

GSM — Global System for Mobile communication

Secura

Mobile

3G rel99 Architecture (UMTS) - 3G Radios



BSS Base Station System

BTS Base Transceiver Station

BSC Base Station Controller

RNS Radio Network System

RNC Radio Network Controller

CN Core Network

MSC Mobile-service Switching Controller

VLR Visitor Location Register

HLR Home Location Register

AuC Authentication Server

GMSC Gateway MSC

SGSN Serving GPRS Support Node

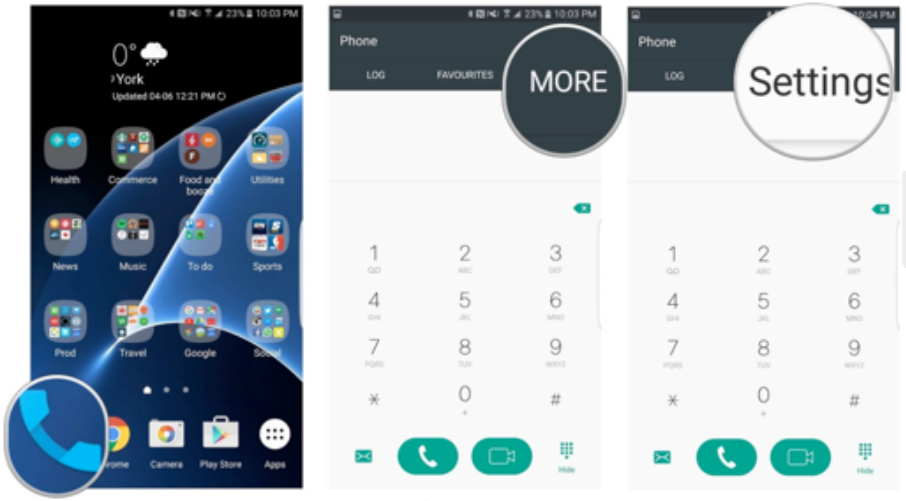
GGSN Gateway GPRS Support Node

UMTS Universal Mobile Telecommunication System

Mobile

Secura

4G



- 4G has a new mode of voice transport: Voice over LTE, VoLTE.
- It is an implementation of VoIP using SIP and RTSP over 4G.
- Signalling is handled in the phone's software (the actual voice path is usually/mostly/always(?) handled by the baseband chip and not available within the Android kernel)
- Signalling therefore back again into the users hand and mistakes from the 70's & 80's also!

Secura

VoLTE

- Android allows interaction with rmnet0 and rmnet1: IP interfaces for data, and SIP (signalling) traffic
- Often rmnet1 is IPv6
- IPsec tunnel is used to connect to SIP proxy (a.k.a. PCFCS)

SECURITY DETAILS

```
root@a3y17lte:/ # ip xfrm policy
src [redacted]:4/128 dst [redacted]:1:2:5789:931c/128 sport 32821 dport 6100
        dir in priority 0
        tmpl src :: dst ::
                proto esp reqid 4 mode transport
src [redacted]:1:2:5789:931c/128 dst [redacted]:4/128 sport 6100 dport 32821
        dir out priority 0
        tmpl src :: dst ::
                proto esp reqid 3 mode transport
```

```
root@a3y17lte:/ # ip xfrm state
src [redacted]:4 dst [redacted]:1:4:9d02:2e42
        proto esp spi 0x000137f8 reqid 4 mode transport
        replay-window 4
        auth-trunc hmac(md5) 0xcad19b13c583c94c8d975d83113aaf4a 96
        enc cbc(des3_ede) 0x4abe8f15fee3719adb5cf91c963cb41b4abe8f15fee3719a
        sel src ::/0 dst ::/0
```

MISCONFIGURATIONS

```
root@a3y17lte:/ # ip xfrm state
src [redacted]:4 dst [redacted]:1:4:9d02:2e42
        proto esp spi 0x000137f8 reqid 4 mode transport
        replay-window 4
        auth-trunc hmac(md5) 0xcad19b13c583c94c8d975d83113aaf4a 96
        enc cbc(des3_ede) 0x4abe8f15fee3719adb5cf91c963cb41b4abe8f15fee3719a
        sel src ::/0 dst ::/0
```

- 3DES Enc key: 192 bits (2/3 = 128 bits)
- 8 bits error correction per key each round (128 – 8*2 = 112 bits)
- Chosen/known-plain text attacks (80 bits, ≈ 1024 bit RSA keys)
- Radio layer also encrypted, but if that fails, then the voice layer is potentially accessible to sophisticated threat actors

MISCONFIGURATIONS

General			
Network IP version	IPv6	IPv4	IPv6
Downgrade IP version?	no	n/a	no
Network discovery	no	yes	no
IPsec			
Authentication type	hmac(md5)	hmac(md5)	hmac(md5)
Authentication key length	128 bits	128 bits	128 bits
Encryption type	ecb(null)	cbc(aes)	cbc(des3_ede)
encryption key length	0 bits	128 bits	192 bits
Disable encryption?	n/a	no	yes
Disable authentication?	no	no	yes
Disable IPsec itself?	no	no	yes

VoLTE sniffing

- Older Android versions use a database with IMS settings:

```
/data/data/com.android.providers.telephony/databases/
/data/data/com.sec.imsservice/databases/
```

- At least one provider allowed disabling of IPsec through hidden activity:

```
am start –n com.samsung.advp.imssettings/.ImsSettingsLauncherActivity
```

Secura

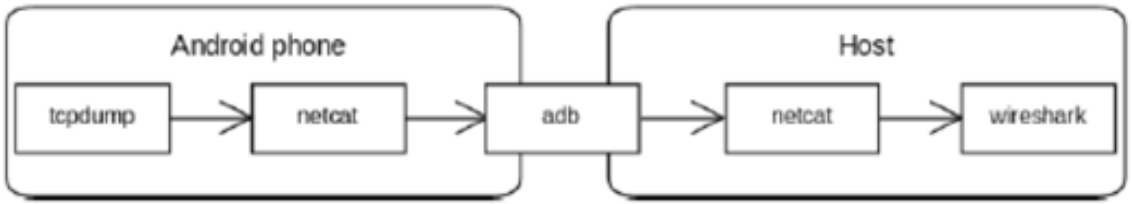
Sniffing traffic

- And if you are root on the phone you can easily extract the IPsec keys:

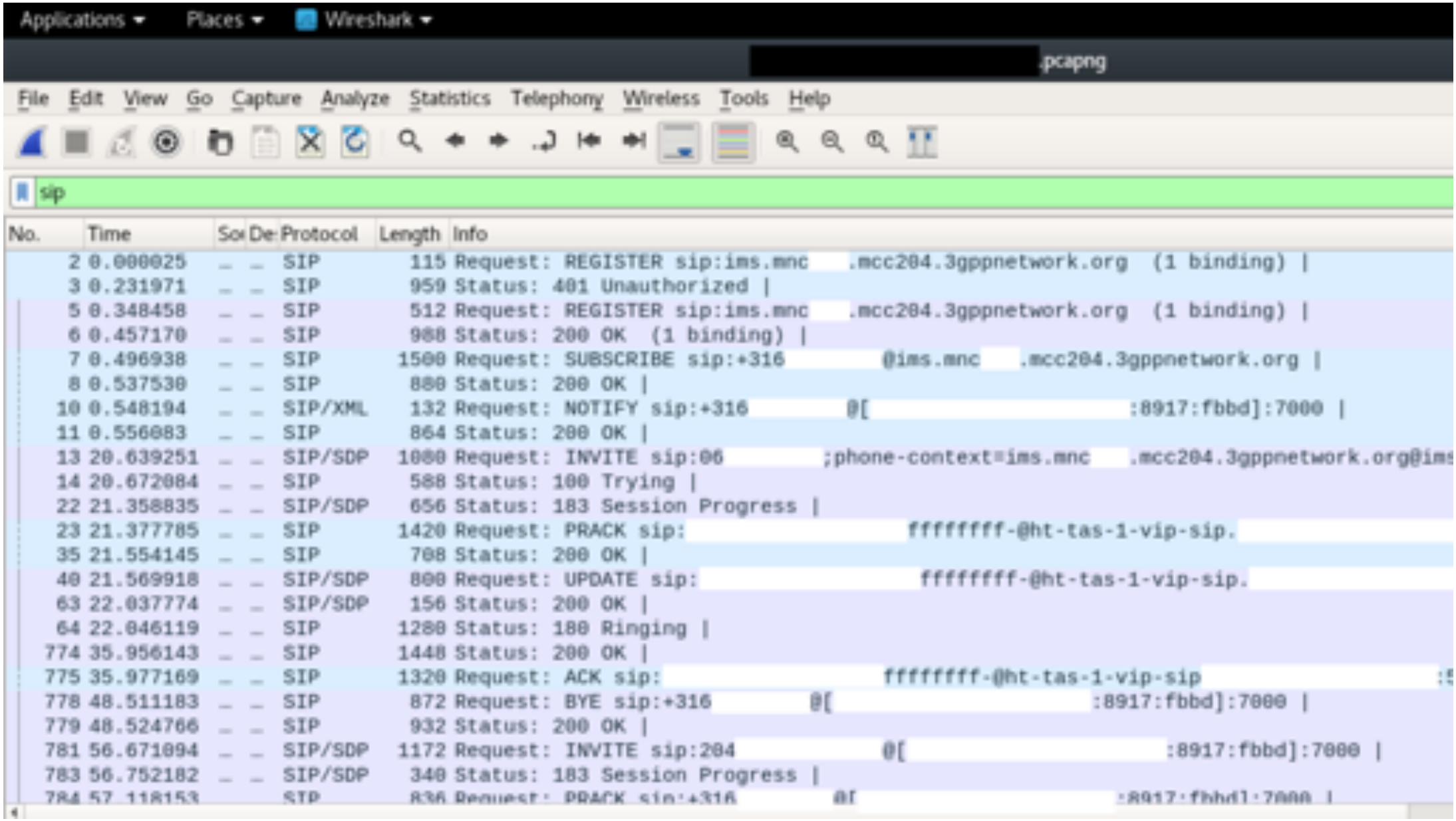
‘`ip xfrm state`’

Sniffing traffic

```
Host:   adb forward tcp:31337 tcp:31337
Device: tcpdump -i any not port 31337 -s 0 -w - | nc -l -p 31337
Host:   nc localhost 31337 | wireshark -i - -k -S
```



Secura


Applications
Places
Wireshark
.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
sip
No. Time Sou Des Protocol Length Info
2 0.000025 _ _ SIP 115 Request: REGISTER sip:ims.mnc .mcc204.3gppnetwork.org (1 binding) |
3 0.231971 _ _ SIP 959 Status: 401 Unauthorized |
5 0.348458 _ _ SIP 512 Request: REGISTER sip:ims.mnc .mcc204.3gppnetwork.org (1 binding) |
6 0.457170 _ _ SIP 988 Status: 200 OK (1 binding) |
7 0.496938 _ _ SIP 1500 Request: SUBSCRIBE sip:+316 @ims.mnc .mcc204.3gppnetwork.org |
8 0.537530 _ _ SIP 880 Status: 200 OK |
10 0.548194 _ _ SIP/XML 132 Request: NOTIFY sip:+316 @[:8917:fbbd]:7000 |
11 0.556083 _ _ SIP 864 Status: 200 OK |
13 20.639251 _ _ SIP/SDP 1080 Request: INVITE sip:06 ;phone-context=ims.mnc .mcc204.3gppnetwork.org@ims
14 20.672084 _ _ SIP 588 Status: 100 Trying |
22 21.358835 _ _ SIP/SDP 656 Status: 183 Session Progress |
23 21.377785 _ _ SIP 1420 Request: PRACK sip: ffffffff-@ht-tas-1-vip-sip.
35 21.554145 _ _ SIP 708 Status: 200 OK |
40 21.569918 _ _ SIP/SDP 800 Request: UPDATE sip: ffffffff-@ht-tas-1-vip-sip.
63 22.037774 _ _ SIP/SDP 156 Status: 200 OK |
64 22.046119 _ _ SIP 1280 Status: 180 Ringing |
774 35.956143 _ _ SIP 1448 Status: 200 OK |
775 35.977169 _ _ SIP 1320 Request: ACK sip: ffffffff-@ht-tas-1-vip-sip :5
778 48.511183 _ _ SIP 872 Request: BYE sip:+316 @[:8917:fbbd]:7000 |
779 48.524766 _ _ SIP 932 Status: 200 OK |
781 56.671094 _ _ SIP/SDP 1172 Request: INVITE sip:204 @[:8917:fbbd]:7000 |
783 56.752182 _ _ SIP/SDP 340 Status: 183 Session Progress |
784 57.118153 SIP 836 Request: PRACK sip:+316 @[:8917:fbbd]:7000 |

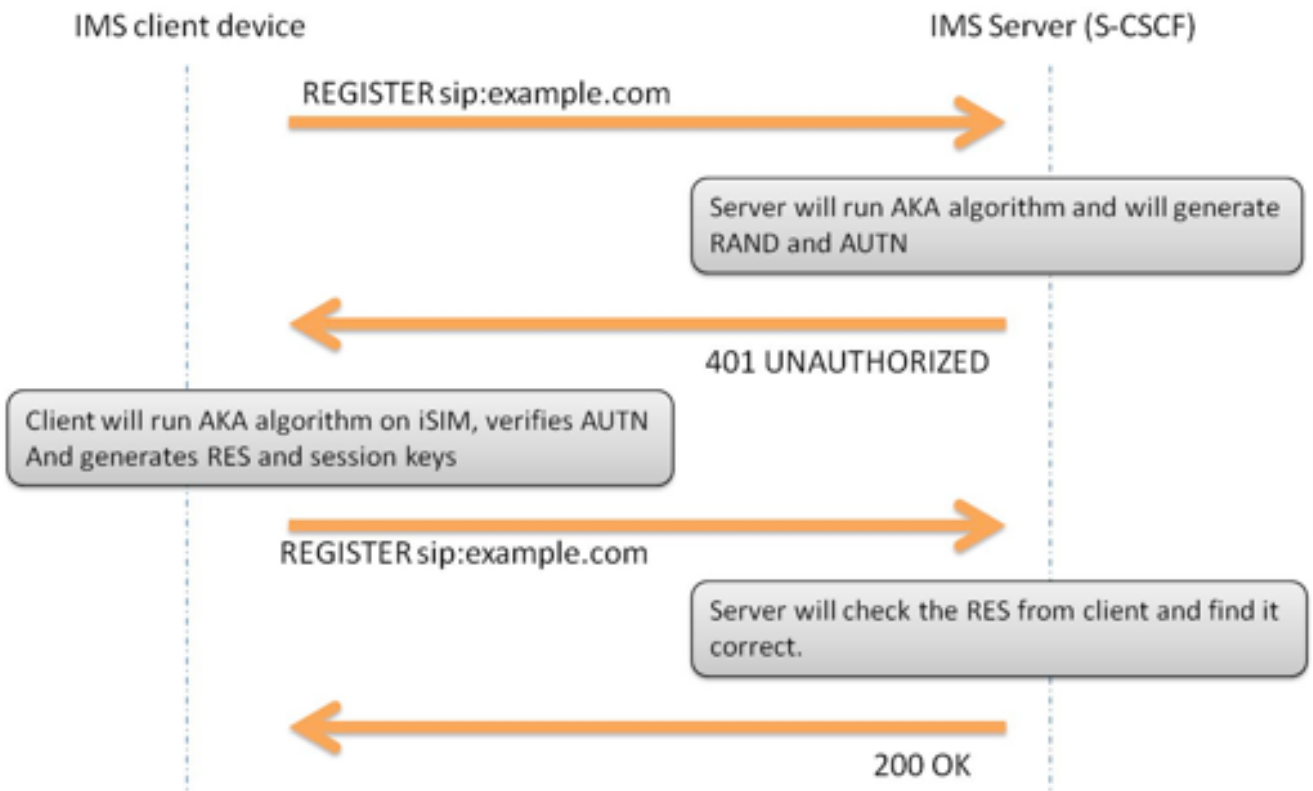
MORE DIFFERENCES

Operator A	Operator B	Operator C	RFC 3261
INVITE	INVITE	INVITE	INVITE
100 Trying	100 Trying	100 Trying	100 Trying
200 OK	183 Session Prog.	183 Session Prog.	180 Ringing
ACK	PRACK	PRACK	200 OK
BYE	200 OK	200 OK	ACK
200 OK	UPDATE	180 Ringing	BYE
	200 OK	200 OK	200 OK
	180 Ringing	ACK	
	200 OK	BYE	
	ACK	200 OK	
	BYE		
	200 OK		

VoLTE data

- Some (non-NL) providers still allow internet access through rmnet1
  - No data charges
  - Tunneling through DNS potentially also an option
  - Infrastructure discovery over rmnet1

VoLTE authentication



Secura

VoLTE SIM sharing

- Send CHALL to other sim-card on other phone over other channel, and receive RESP, and authenticate as that one
- Multiple users can share SIM-card that way
- Lawful interception and attribution at risk
- Theoretical: not tested yet (confident in feasability through)

Secura

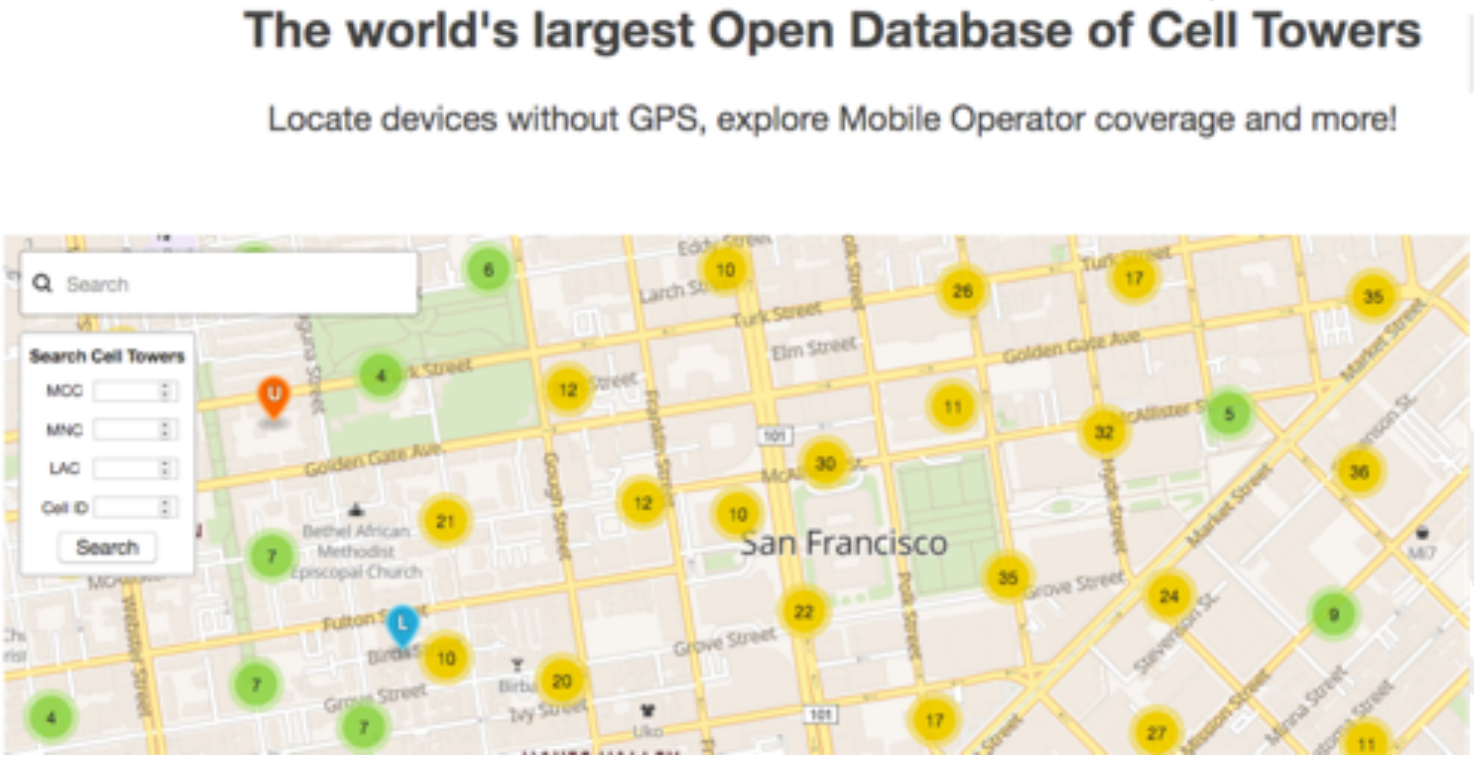
VoLTE SMS

- Not all providers use this
- But tricks were possible in at least one implementation:
  - Replay SMS (SIP MESSAGE) from other phone
  - Network thinks SMS is from original phone (and bills him/her)
  - Enumerate users (errors generated if recipient not known)

VoLTE Leakage

- In at least one implementation, SIP traffic revealed too much information: `P-Access-Network-Info` header has `utran-cell-id-3gpp=20x0xabcd1234567` of call recipient.

VoLTE Leakage



Secura

VoLTE Leakage

- Under certain conditions, called ID blocking is ignored:
  - #31# private calls are revealed anyway in SIP headers
  - Also IP addresses of call recipients
  - And IMEI of recipient

- When aborting call without other side ringing, this info is received (stealthy) in SIP PROGRESS message

Secura

VoLTE has a cousin

- VoWiFi
- Same functionality over WiFi

Secura

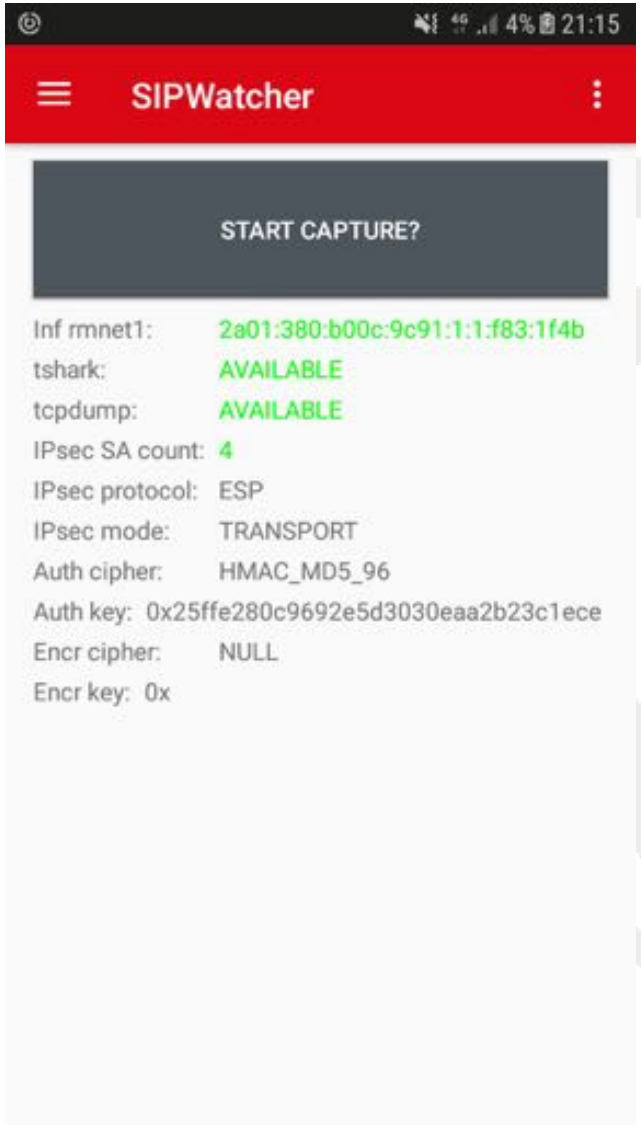
SIPWatcher

- Berry Busser wrote an app to monitor SIP traffic
- https://github.com/SecuraBV/SIPWatcher
- No guarantees, Open Source, As-is
- Under limited development, contributions welcome!
- Known to work on Samsung A3 (other models will follow)
- If you are able to run it in other countries on other providers, we are interested in the results!

Secura

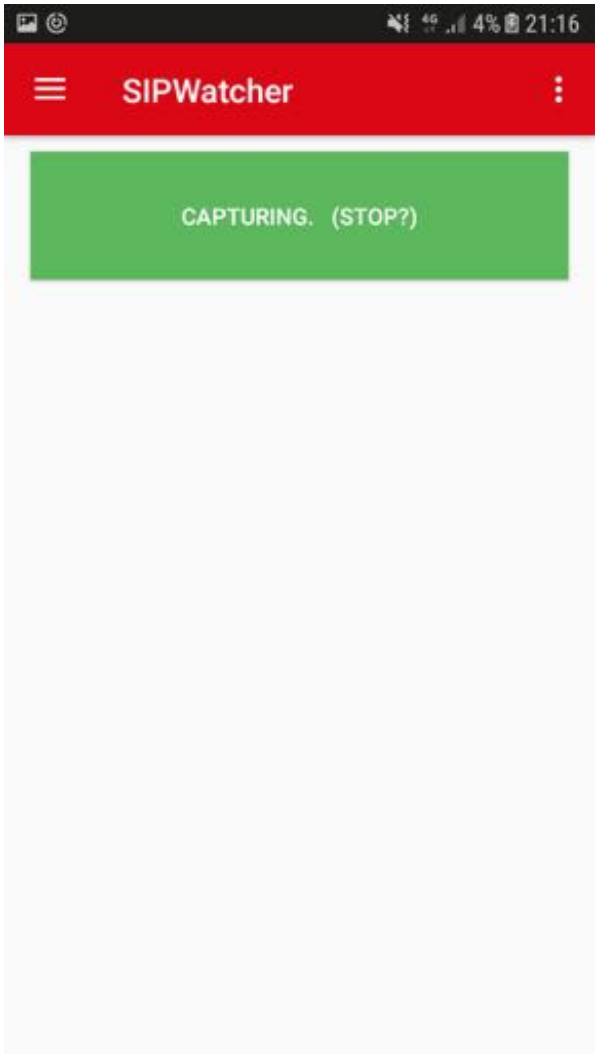
SIPWatcher

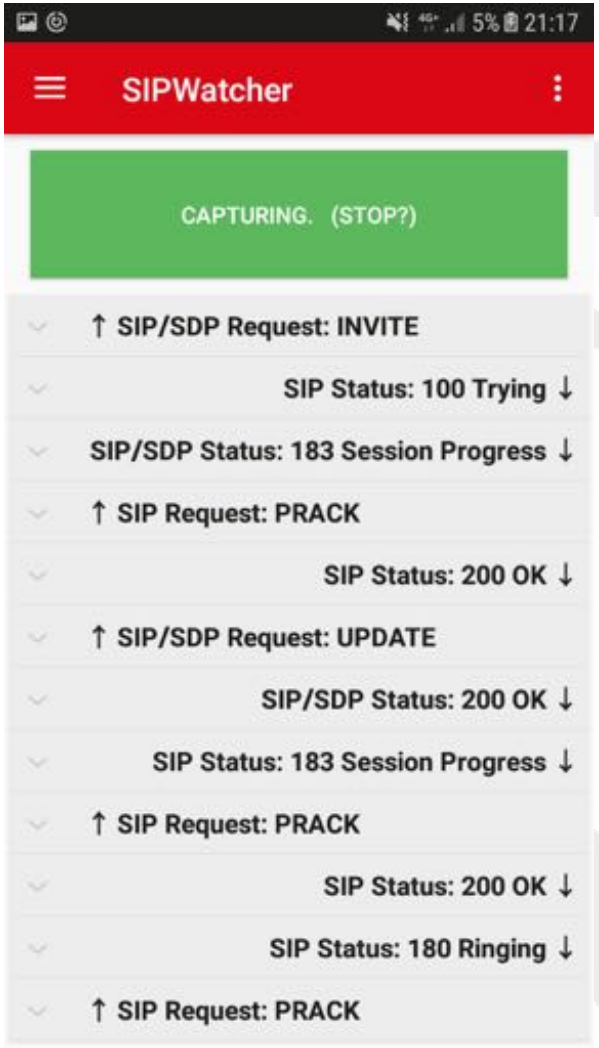
- Uses tcpdump and tshark to sniff and decode from rmnet1
- armv8 version included in .apk
- Needs to be crosscompiled for other architectures (tbd)



Secura

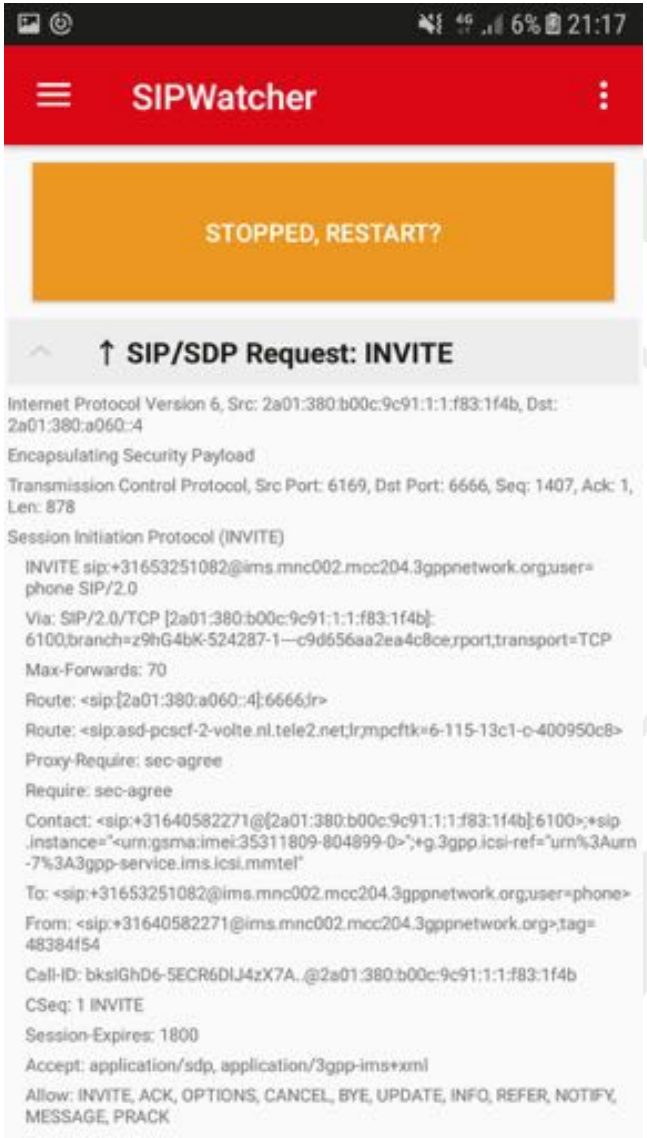
SIPWatcher





Secura

SIPWatcher



Secura

Conclusions

- Phreaking is back in 2019, in a digital way
- Possible, because signalling back in the hands of the user
- Already weaknesses are being found:
  - SMS spoofing, card sharing, subscriber locating, privacy issues.

Secura

Some notes

- Legality: interaction with operator's network might be illegal.
- Simple observation of your own traffic is legal in most countries.
- Based in part on work by Berry Busser, Radboud Uni, that he did for Secura as his Master Thesis.
- Responsible disclosure was followed in all cases, mentioned issues have been mostly remediated in NL for relevant providers.

Secura

FOLLOW US ON

Secura

© 2018. Proprietary & Confidential.