4G Voice communications hacking (a.k.a. Phreaking in 2018)

OWASP BeNeLux-Days 2018

Secura

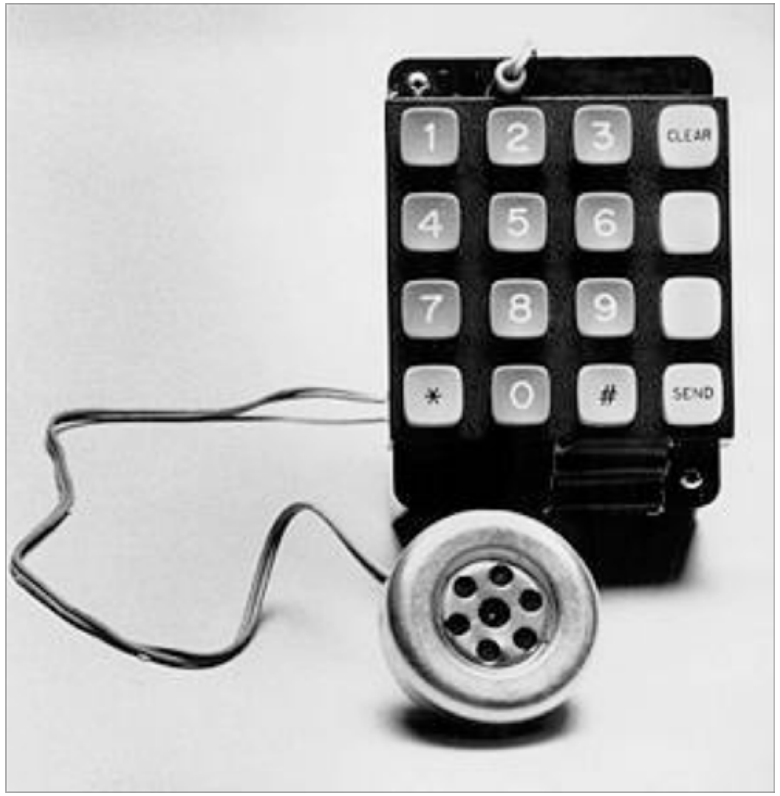
Who am I?

- 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 2018
- Vulnerabilities discovered: some new, some old

History



Secura

History

- Signalling systems
  - Like DTMF but other frequencies
  - Could be heard while setting up call
  - Can also be injected by end-user
  - Trick exchange into thinking end-user is also exchange
  - R1, R2, CCITT4, CCITT5
  - ftp://ftp.wideweb.com/GroupBell

History in NL

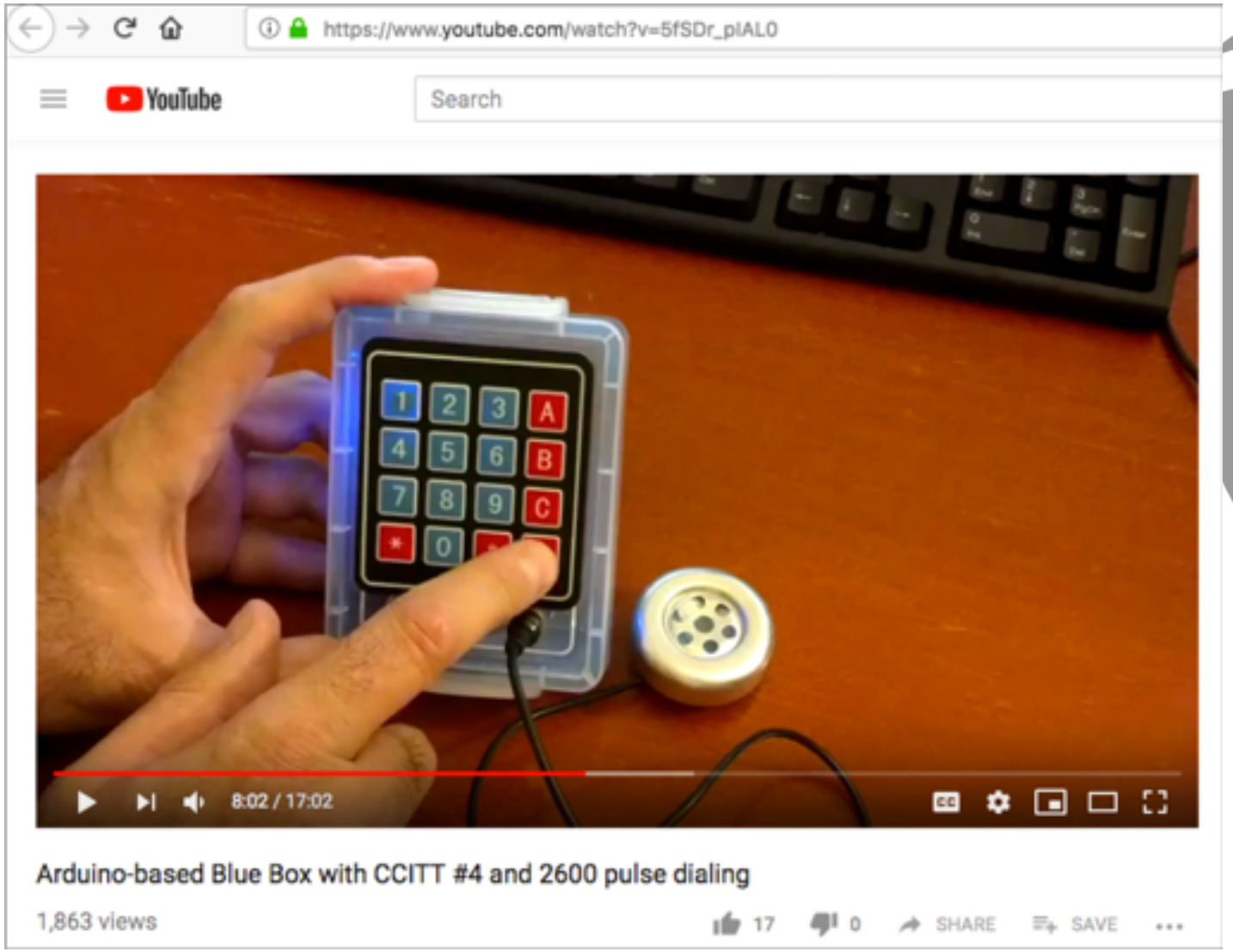
- 80’s: a group in NL found that this also worked here.
- Back then, 06-022XXXX where toll-free (now 0800-numbers)
- Often international lines: faxes, hotel reservations, modems, etc.
- Allowed phreaking!

Secura

History in NL

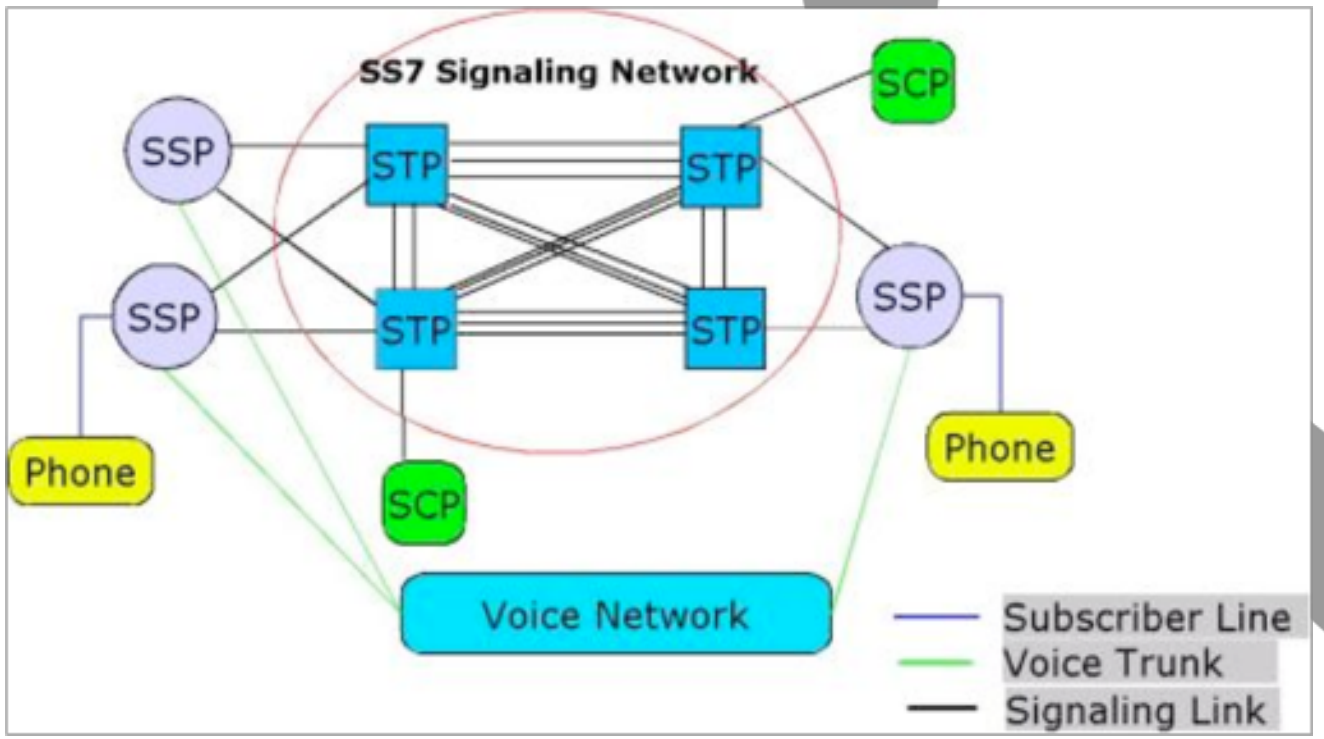
- Blue box, brown box, green box: the rainbow warrior
- Endless phun!
- Make phree phone calls, get connected to chatrooms, secret switchboards, operators in Korea, the White House, CIA, FBI, and lots of modems.
- Remember: dial-in lines were expensive

Play around yourself



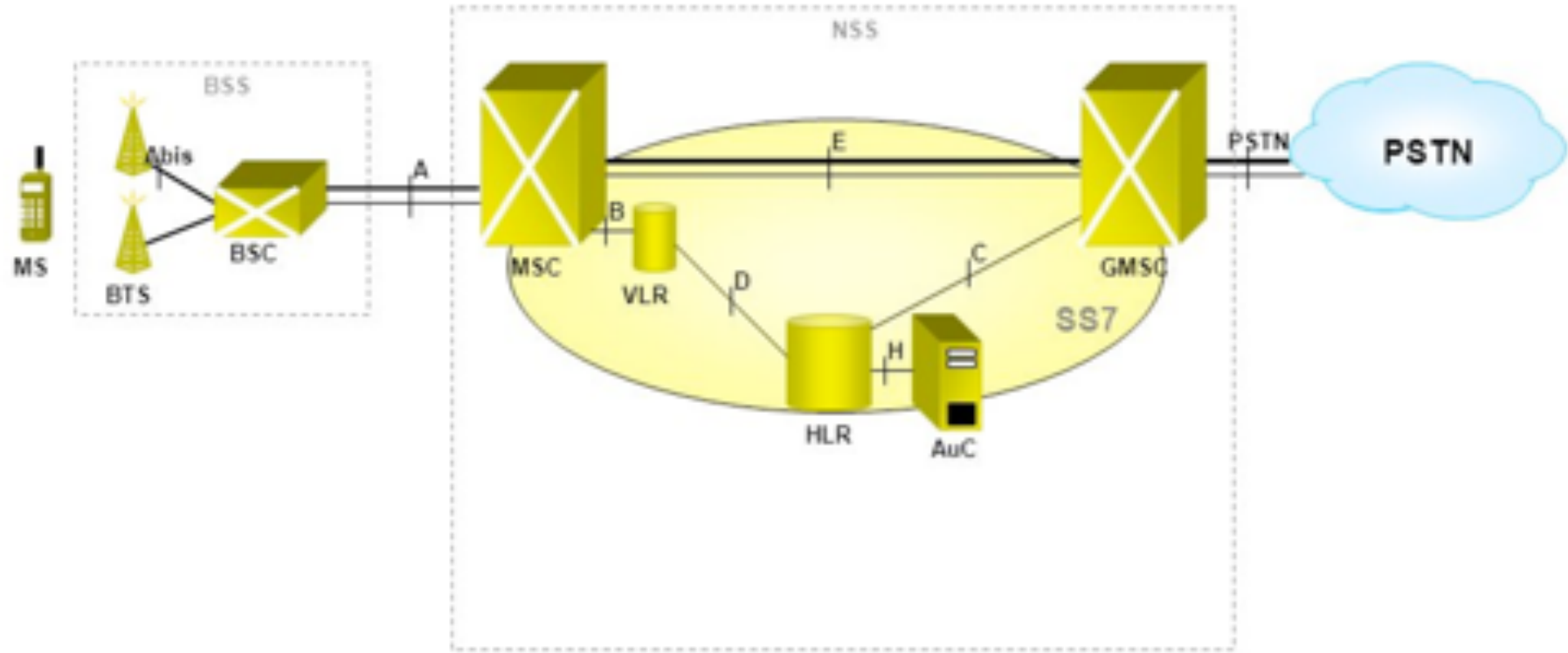
Digital

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



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

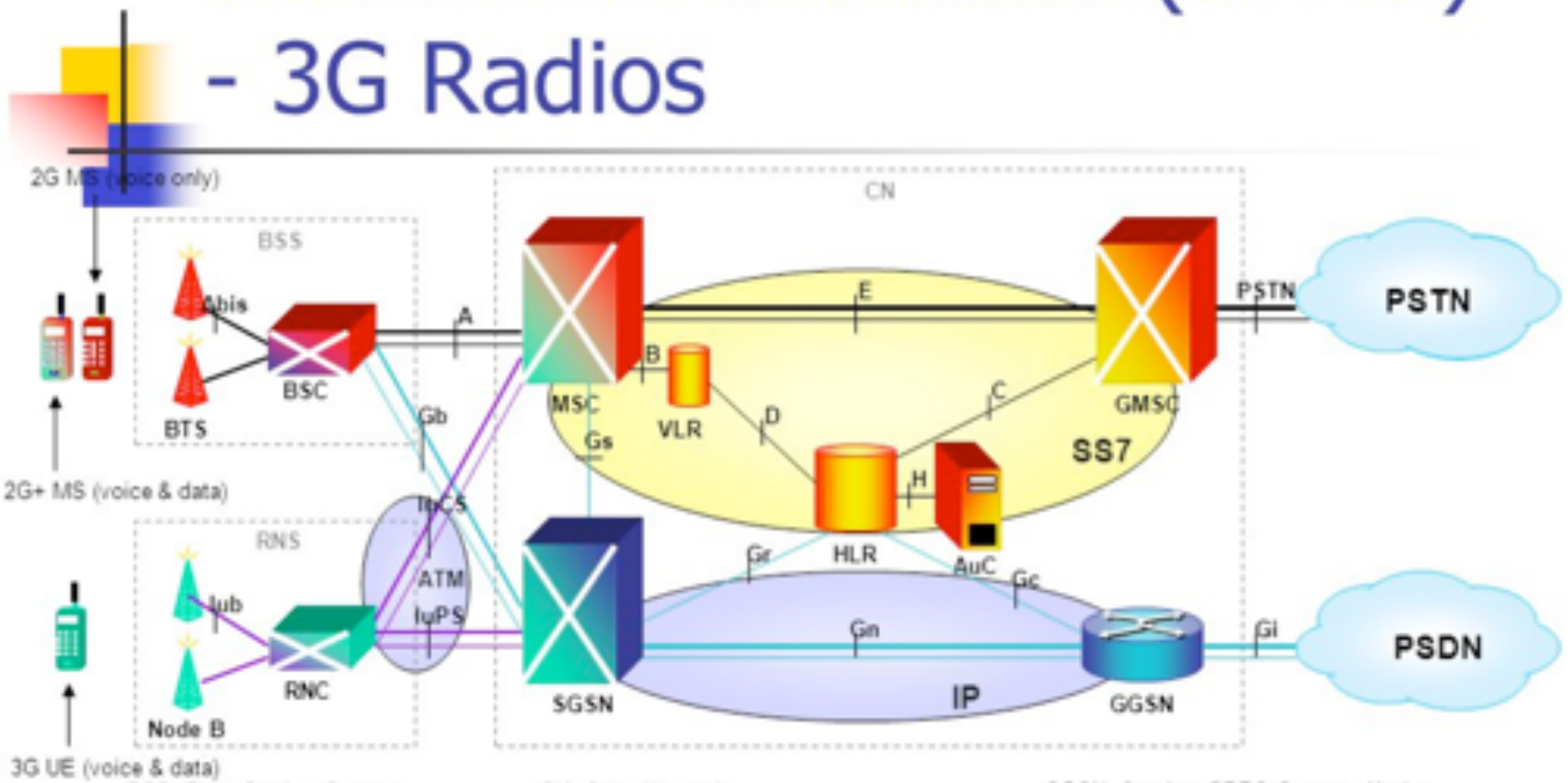
GMSC — Gateway MSC

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

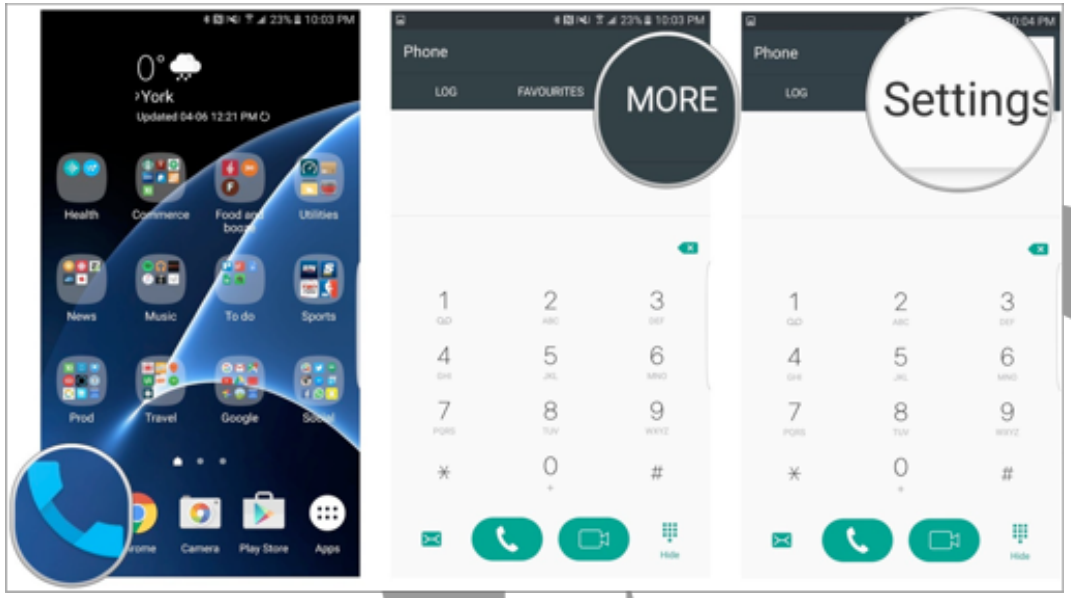
UMTS Universal Mobile Telecommunication System

Secura

Mobile

Secura

4G



- 4G has a new mode of voice transport: Voice over LTE, VoLTE.
- It is an implementation of VoIP using SIP
- Signalling is handled in the phone's software (the actual voice is handled by the baseband chip)
- 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 traffic
- Often rmnet1 is IPv6
- IPsec tunnel is used to connect to SIP proxy

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

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
```

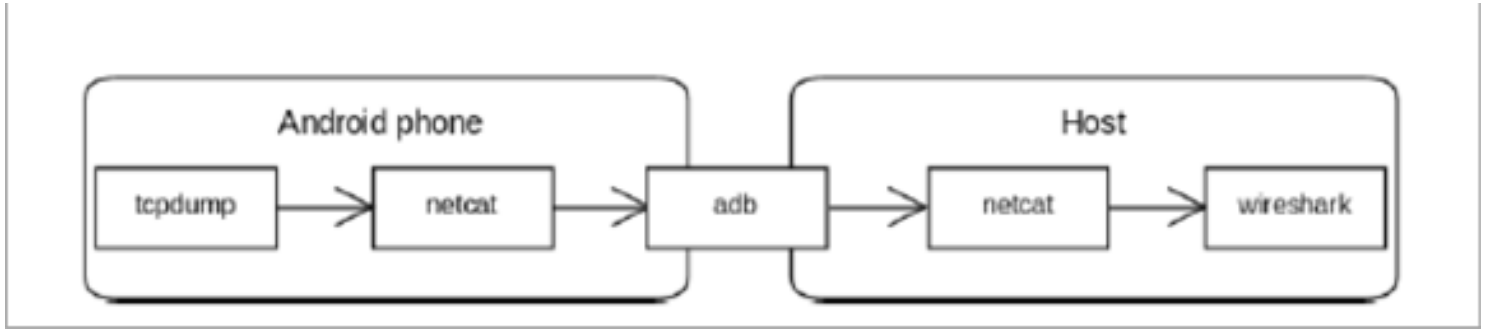
3DES Enc key: 192 bits (2/3 = 128 bits)

8 bits error correction per key each round (128 – 8*2 = 112 bits)

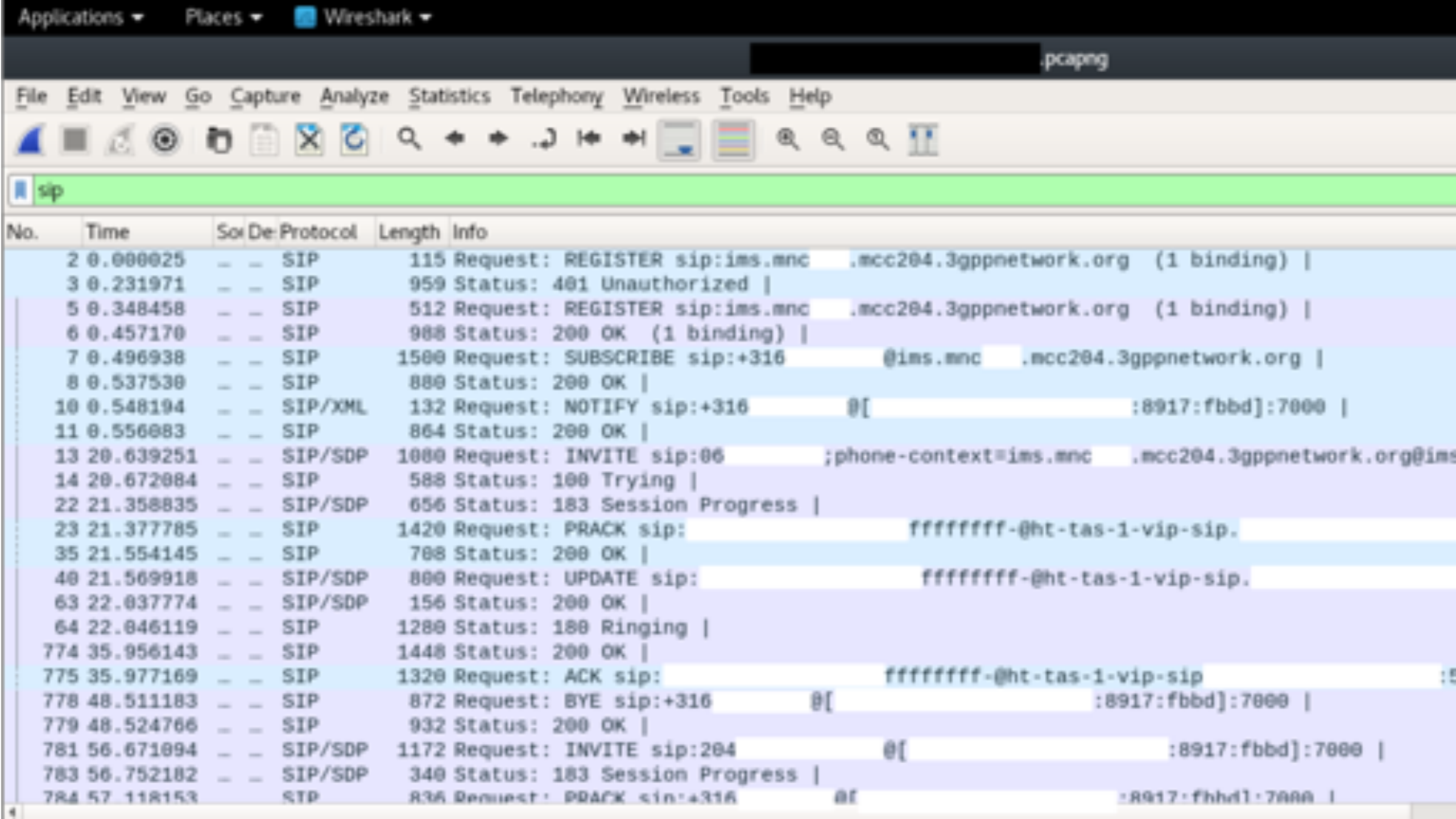
Chosen/known-plain text attacks (80 bits, ≈ 1024 bit RSA keys)

VoLTE sniffing

- Some providers might allow disabling of IPsec
- But if you are root on the phone:



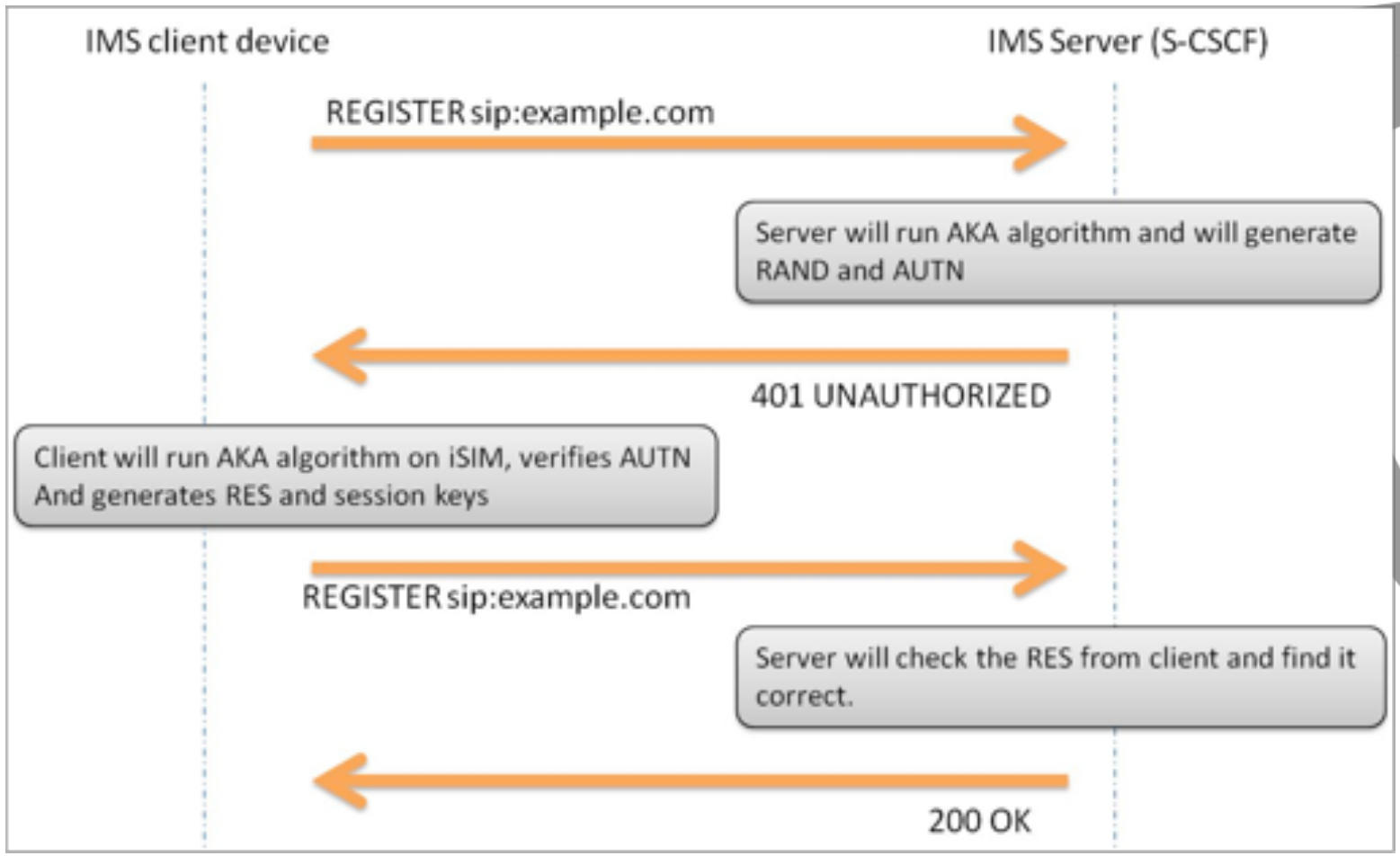
- ‘`ip xfrm state`’ dumps ipsec keys


Applications
Places
Wireshark
[redacted].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 |

VoLTE data

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

VoLTE authentication



Secura

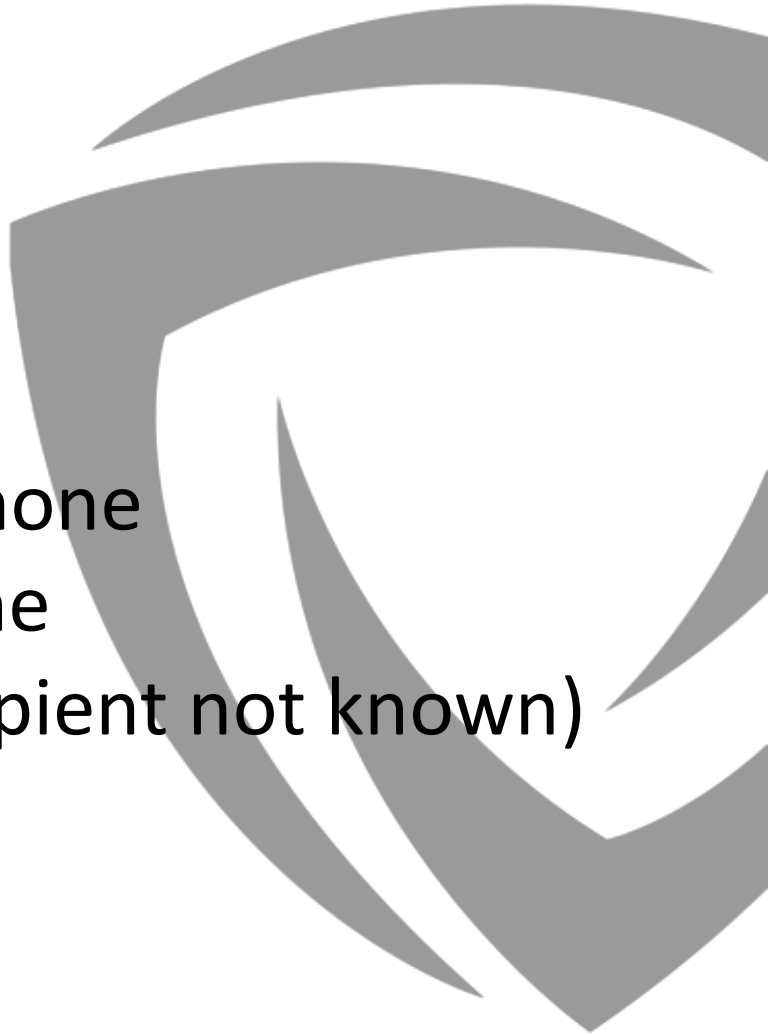
VoLTE SIM sharing

- Send CHALL to other sim-card on other phone, and authenticate as him
- Multiple users can share SIM-card that way
- Lawful interception and attribution at risk

Secura

VoLTE SMS

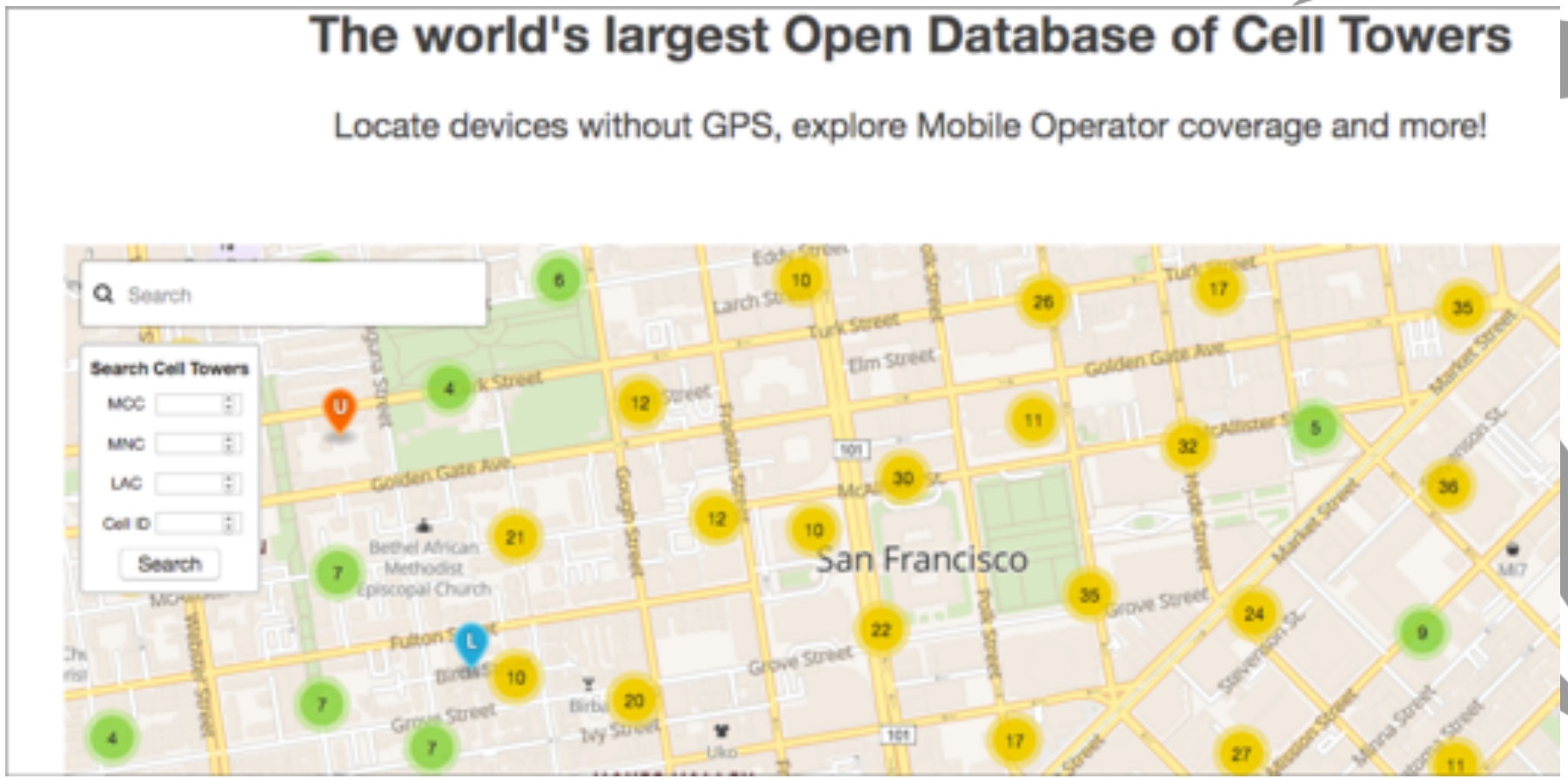
- Not all providers use this
- But tricks are possible sometimes:
  - Replay SMS (SIP MESSAGE) from other phone
  - Network thinks SMS is from original phone
  - Enumerate users (errors generated if recipient not known)



VoLTE Leakage

- Under certain conditions, SIP traffic can reveal too much information: `P-Access-Network-Info` header has `utran-cell-id-3gpp=20x0xabcd1234567`

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

- Also when aborting call, this info is received (stealthy)

VoLTE has a cousin

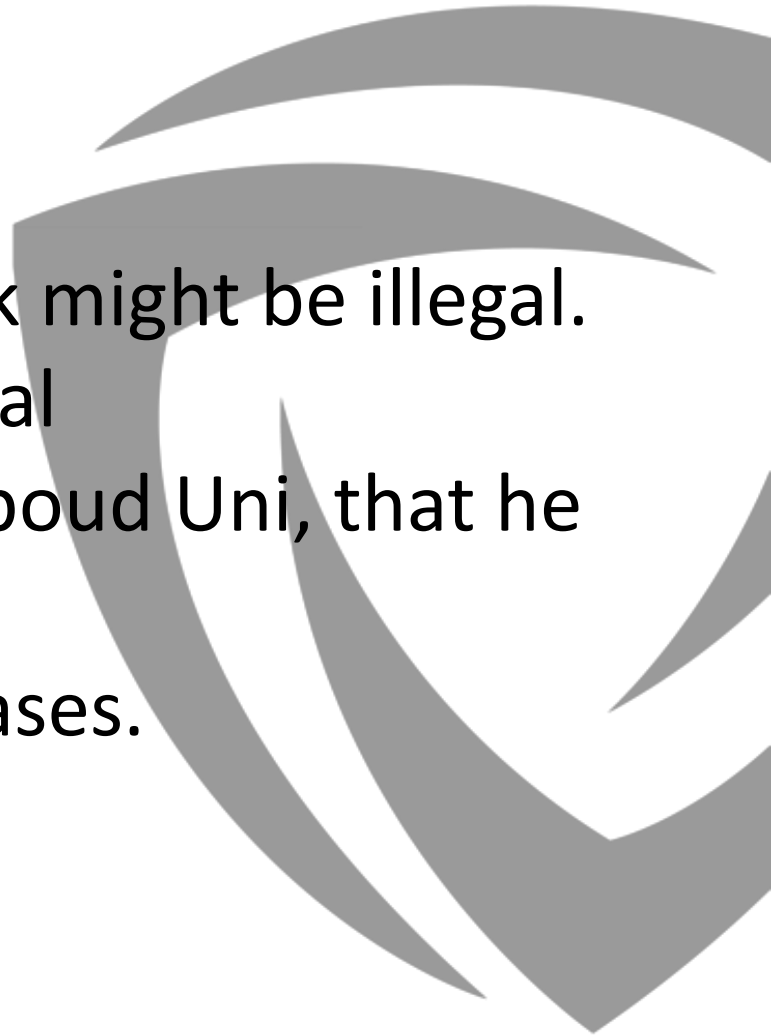
- VoWiFi
- Same functionality over WiFi

Conclusions

- Phreaking is back in 2018, 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.

Some notes

- Legality: interaction with operator's network might be illegal.
- Simple observation of your own traffic is legal
- Based partly on work by Berry Bussers, Radboud Uni, that he did for us as his Master Thesis.
- Responsible disclosure was followed in all cases.



FOLLOW US ON

Secura