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
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!
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

https://www.youtube.com/watch?v=5fSdr_piAL0

Arduino-based Blue Box with CCITT #4 and 2600 pulse dialing

1,863 views
Digital

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

PSTN Public Switched Telephone Network
PSDN Public Switched Data Network

UMTS Universal Mobile Telecommunication System
Mobile
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!
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 dir in priority 0
  tmpl src :: dst ::
    proto esp reqid 4 mode transport
src dir out priority 0
  tmpl src :: dst ::
    proto esp reqid 3 mode transport

root@a3y17lte:/> # ip xfrm state
src 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

- 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

<table>
<thead>
<tr>
<th>General</th>
<th>IPv6</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network IP version</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Downgrade IP version?</td>
<td>no</td>
<td>n/a</td>
<td>no</td>
</tr>
<tr>
<td>Network discovery</td>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPsec</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication type</td>
<td>hmac(md5)</td>
<td>hmac(md5)</td>
<td>hmac(md5)</td>
</tr>
<tr>
<td>Authentication key length</td>
<td>128 bits</td>
<td>128 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td>Encryption type</td>
<td>ecb(null)</td>
<td>cbc(aes)</td>
<td>cbc(des3_ede)</td>
</tr>
<tr>
<td>Encryption key length</td>
<td>0 bits</td>
<td>128 bits</td>
<td>192 bits</td>
</tr>
<tr>
<td>Disable encryption?</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Disable authentication?</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Disable IPsec itself?</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
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
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
<table>
<thead>
<tr>
<th>No</th>
<th>Time</th>
<th>Source/Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.000025</td>
<td>SIP</td>
<td>115</td>
<td>Request: REGISTER sip:ims.mnc.mcc204.3gppnetwork.org (1 binding)</td>
</tr>
<tr>
<td>3</td>
<td>0.231971</td>
<td>SIP</td>
<td>959</td>
<td>Status: 401 Unauthorized</td>
</tr>
<tr>
<td>5</td>
<td>0.348458</td>
<td>SIP</td>
<td>512</td>
<td>Request: REGISTER sip:ims.mnc.mcc204.3gppnetwork.org (1 binding)</td>
</tr>
<tr>
<td>6</td>
<td>0.457170</td>
<td>SIP</td>
<td>980</td>
<td>Status: 200 OK (1 binding)</td>
</tr>
<tr>
<td>7</td>
<td>0.496938</td>
<td>SIP</td>
<td>1500</td>
<td>Request: SUBSCRIBE sip:<a href="mailto:+316@ims.mnc.mcc204.3gppnetwork.org">+316@ims.mnc.mcc204.3gppnetwork.org</a></td>
</tr>
<tr>
<td>8</td>
<td>0.537530</td>
<td>SIP</td>
<td>880</td>
<td>Status: 200 OK</td>
</tr>
<tr>
<td>9</td>
<td>0.548194</td>
<td>SIP/SDP</td>
<td>132</td>
<td>Request: NOTIFY sip:+316@[:8917:ffbd]:7000</td>
</tr>
<tr>
<td>10</td>
<td>0.556083</td>
<td>SIP</td>
<td>864</td>
<td>Status: 200 OK</td>
</tr>
<tr>
<td>13</td>
<td>20.639251</td>
<td>SIP/SDP</td>
<td>1000</td>
<td>Request: INVITE sip:06;phone-context=ims.mnc.mcc204.3gppnetwork.org</td>
</tr>
<tr>
<td>14</td>
<td>20.672084</td>
<td>SIP</td>
<td>588</td>
<td>Status: 100 Trying</td>
</tr>
<tr>
<td>22</td>
<td>21.358835</td>
<td>SIP/SDP</td>
<td>656</td>
<td>Status: 183 Session Progress</td>
</tr>
<tr>
<td>23</td>
<td>21.577785</td>
<td>SIP</td>
<td>1420</td>
<td>Request: PRACK sip:fffffffff@ht-tas-1-vip-sip</td>
</tr>
<tr>
<td>35</td>
<td>21.554145</td>
<td>SIP</td>
<td>708</td>
<td>Status: 200 OK</td>
</tr>
<tr>
<td>40</td>
<td>21.569918</td>
<td>SIP/SDP</td>
<td>800</td>
<td>Request: UPDATE sip:fffffffff@ht-tas-1-vip-sip</td>
</tr>
<tr>
<td>63</td>
<td>22.037774</td>
<td>SIP/SDP</td>
<td>156</td>
<td>Status: 200 OK</td>
</tr>
<tr>
<td>64</td>
<td>22.046119</td>
<td>SIP</td>
<td>1280</td>
<td>Status: 180 Ringing</td>
</tr>
<tr>
<td>774</td>
<td>35.977169</td>
<td>SIP</td>
<td>1440</td>
<td>Status: 200 OK</td>
</tr>
<tr>
<td>775</td>
<td>35.977169</td>
<td>SIP</td>
<td>1320</td>
<td>Request: ACK sip:fffffffff@ht-tas-1-vip-sip</td>
</tr>
<tr>
<td>778</td>
<td>48.511183</td>
<td>SIP</td>
<td>872</td>
<td>Request: BYE sip:+316@[:8917:ffbd]:7000</td>
</tr>
<tr>
<td>779</td>
<td>48.524766</td>
<td>SIP</td>
<td>932</td>
<td>Status: 200 OK</td>
</tr>
<tr>
<td>781</td>
<td>56.671094</td>
<td>SIP/SDP</td>
<td>1172</td>
<td>Request: INVITE sip:204@[:8917:ffbd]:7000</td>
</tr>
<tr>
<td>783</td>
<td>56.752182</td>
<td>SIP/SDP</td>
<td>340</td>
<td>Status: 183 Session Progress</td>
</tr>
<tr>
<td>784</td>
<td>57.118153</td>
<td>SIP</td>
<td>836</td>
<td>Request: PRACK sip:+316@[:8917:ffbd]:7000</td>
</tr>
</tbody>
</table>
MORE DIFFERENCES

<table>
<thead>
<tr>
<th>Operator A</th>
<th>Operator B</th>
<th>Operator C</th>
<th>RFC 3261</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE</td>
<td>INVITE</td>
<td>INVITE</td>
<td>INVITE</td>
</tr>
<tr>
<td>100 Trying</td>
<td>100 Trying</td>
<td>100 Trying</td>
<td>100 Trying</td>
</tr>
<tr>
<td>200 OK</td>
<td>183 Session Prog.</td>
<td>183 Session Prog.</td>
<td>180 Ringing</td>
</tr>
<tr>
<td>ACK</td>
<td>PRACK</td>
<td>PRACK</td>
<td>200 OK</td>
</tr>
<tr>
<td>BYE</td>
<td>200 OK</td>
<td>200 OK</td>
<td>ACK</td>
</tr>
<tr>
<td>200 OK</td>
<td>UPDATE</td>
<td>180 Ringing</td>
<td>BYE</td>
</tr>
<tr>
<td>200 OK</td>
<td>180 Ringing</td>
<td>200 OK</td>
<td>200 OK</td>
</tr>
<tr>
<td>180 Ringing</td>
<td></td>
<td>ACK</td>
<td></td>
</tr>
<tr>
<td>200 OK</td>
<td></td>
<td>BYE</td>
<td></td>
</tr>
<tr>
<td>ACK</td>
<td></td>
<td>200 OK</td>
<td></td>
</tr>
<tr>
<td>BYE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 OK</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

IMS client device

REGISTER sip:example.com

IMS Server (S-CSCF)

Server will run AKA algorithm and will generate RAND and AUTN

401 UNAUTHORIZED

Client will run AKA algorithm on iSIM, verifies AUTN and generates RES and session keys

REGISTER sip:example.com

Server will check the RES from client and find it correct.

200 OK
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 feasibility through)
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

The world's largest Open Database of Cell Towers
Locate devices without GPS, explore Mobile Operator coverage and more!
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
VoLTE has a cousin

- VoWiFi
- Same functionality over WiFi
SIPWatcher

• Berry Busser wrote an app to monitor SIP traffic
• [https://github.com/SecuraBV/SIPWatcher](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!
SIPWatcher

- Uses tcpdump and tshark to sniff and decode from rmnet1
- armv8 version included in .apk
- Needs to be crosscompiled for other architectures (tbd)
SIPWatcher
SIPWatcher has been granted superuser permissions for an interactive shell.
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.
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.