$ 600 Billion
Some Numbers

- $600 Billion
- 90% of population has coverage
Some Numbers

- $600 Billion
- 90% of population has coverage
- 4.1 billion mobile users
$ 600 Billion
90% of population has coverage
4.1 billion mobile users

But has GSM been properly tested?
Cellular technology
The Um interface
Software Defined Radio

- USRP
- Gnu Radio
- Air Probe

Have these new SDR products made GSM less secure?
Software Defined Radio

- USRP
- Gnu Radio
  - Air Probe

Have these new SDR products made GSM less secure?
Software Defined Radio

- USRP
- Gnu Radio
- Air Probe

Have these new SDR products made GSM less secure?
• USRP
• Gnu Radio
• Air Probe

Have these new SDR products made GSM less secure?
and then....

**de Volkskrant**
GSM-encryptie gekraakt

**The New York Times**
Cellphone Encryption Code Is Divulged

**cnet.com**
Cracking GSM phone crypto via distributed computing

**Physorg.com**
Guide to breaking cell phone security revealed

**PCWorld**
Hackers Show It's Easy to Snoop on a GSM Call

**The Register**
Secret code protecting cellphone calls set loose
Universal phone snooping moves forward
The Um interface
Frequency band (GSM900)

- 890.0 MHz
- 960.0 MHz
- 70 MHz
Frequency band (II)

- 960.0 MHz
- 925.0 MHz
- 915.0 MHz
- 890.0 MHz
Frequency band (III)
Frequency band (III)
Frequency division
Combined up and down link frequency
Frequency division

{1, 10, 74, 96}
{17, 69, 77, 94}
{7, 8, 14, 83}
{1, 67, 95, 102}

{5, 16, 83, 100}
Frequency division

\{17, 69, 77, 94\}
GSM messages

49 06 1b 32 22 02 f4 80 – 11 7f d8 04 28 15 65 04 – a9 00 00 1c 13 2b 2b

55 06 19 00 00 00 00 20 – 00 10 10 00 00 00 00 00 – 01 00 00 a9 00 00 2b
KPN system information

1: 49 06 1b 32 22 02 f4 80 – 11 7f d8 04 28 15 65 04 – a9 00 00 1c 13 2b 2b
  0: 49 010010-- Pseudo Length: 18
  1: 06 0------- Direction: From originating site
  1: 06 -000---- 0 TransactionID
  1: 06 -----0110 Radio Resource Management
  2: 1b 00011011 RRsystemInfo3C
  3: 32 12834 [0x3222] Cell identity
  5: 02 204 Mobile Country Code (Netherlands)
  6: f4 08f Mobile Network Code (KPN Telecom B.V.)
  8: 11 4479 [0x117f] Local Area Code
 10: d8 1------- Spare bit (should be 0)
 10: d8 --011--- Number of blocks: 3
 10: d8 -----000 1 basic physical channel for CCCH, not combined with SDCCHs
 11: 04 00000-- spare bits (should be 0)
 11: 04 -----100 6 multi frames period for paging request
 12: 28 00101000 T3212 TimeOut value: 40
 13: 15 0------- spare bit (should be 0)
 13: 15 -----000 Power control indicator is not set
 13: 15 --01---- MSs shall use uplink DTX
 13: 15 -----0101 Radio Link Timeout: 24
 14: 65 011----- Cell Reselect Hyst.: 6 db RXLEV
 14: 65 -----xxxxx Max Tx power level: 5
 15: 04 0------- No additional cells in SysInfo 7–8
 15: 04 -----00 New establishm cause: not supported
 15: 04 -----xxxxx RXLEV Access Min permitted = –110 + 4dB
 16: a9 10------- Max. of retransmiss : 4
 16: a9 --1010-- slots to spread TX : 14
 16: a9 ------0-- The cell is barred : no
 16: a9 -------1 Cell reestabl.i.cell: not allowed
 17: 00 ------0-- Emergency call EC 10: allowed
 17: 00 00000-- Acc ctrl cl 11–15: 0 = permitted, 1 = forbidden
 17: 00 ------00 Acc ctrl cl 8– 9: 0 = permitted, 1 = forbidden
 17: 00 ------0 Ordinary subscribers (8)
 17: 00 -------0 Ordinary subscribers (9)
KPN system information

2: 55 06 19 00 00 00 00 20 – 00 10 10 00 00 00 00 – 01 00 00 a9 00 00 2b
0: 55 010101-- Pseudo Length: 21
1: 06 0-------- Direction: From originating site
1: 06 –000---- 0 TransactionID
1: 06 -----0110 Radio Resource Management
2: 19 00011001 RRsystemInfo1
3: 00 00-------- Bitmap 0 format
7: 20 --1------ Cell Allocation : ARFCN 94
9: 00000000

7: 20 --1------ Cell Allocation : ARFCN 77
10: 00000000

10: 00000000

16: 01 -------1 Cell Allocation : ARFCN 69
19: a9 10------ Max. of retransmission : 4
19: a9 --1010-- slots to spread TX : 14
19: a9 --------0 The cell is barred : no
19: a9 --------1 Cell reestabl.i.cell: not allowed
20: 00 -------0-- Emergency call EC 10: allowed
20: 00 00000--- Acc ctrl cl 11–15: 0 = permitted, 1 = forbidden
20: 00 00000--- Acc ctrl cl 8–9: 0 = permitted, 1 = forbidden
20: 00 --------0 Ordinary subscribers (8)
20: 00 --------0 Ordinary subscribers (9)
20: 00 --------0-- Emergency call (10): Everyone
20: 00 ----0--- Operator Specific (11)
20: 00 ----0--- Security service (12)
20: 00 -----0--- Public service (13)
20: 00 00000000 Emergency service (14)
20: 00 00000000 Network Operator (15)
21: 00 00000000 Acc ctrl cl 0–7: 0 = permitted, 1 = forbidden
21: 00 00000000 Ordinary subscribers (0–7)
KPN system information

[0x3222] Cell identity
  Mobile Country Code (Netherlands)
  Mobile Network Code (KPN Telecom B.V.)
[0x117f] Local Area Code

Cell Allocation: ARFCN 94
Cell Allocation: ARFCN 77
Cell Allocation: ARFCN 69
Cell Allocation: ARFCN 17
The KPN cell

\{17, 69, 77, 94\}
The KPN cell
No Frequency hopping
Frequency hopping (I)
Frequency hopping (II)
<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0: 31 001100</td>
<td>Pseudo Length: 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1: 06 0------</td>
<td>Direction: From originating site</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1: 06 000-----</td>
<td>0 TransactionID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1: 06 00110</td>
<td>Radio Resource Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2: 3f 011111</td>
<td>RRimmediateAssignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2: 3f x------</td>
<td>Send sequence number: 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3: 00 --------00</td>
<td>Page Mode: Normal paging</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3: 00 0-------</td>
<td>No meaning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3: 00 00------</td>
<td>Downlink assign to MS: No meaning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3: 00 000-----</td>
<td>This messages assigns a dedicated mode resource</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4: 52 0010--</td>
<td>Timeslot number: 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4: 52 01010---</td>
<td>Chan. Descript.: SDCCH/8 + SACCH/C8 or CBCH (SDCCH/8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5: f0 111-----</td>
<td>Training seq. code : 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5: f0 01-----</td>
<td>HoppingChannel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6: ab --------</td>
<td>Mobile Allocation Index Offset (MAIO) 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6: ab --101011</td>
<td>Hopping Seq. Number: 43</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7: 85 100-----</td>
<td>Establishing Cause: Answer to paging</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7: 85 000000</td>
<td>Random Reference : 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8: ad xxxxxxx</td>
<td>T1/T2/T3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9: e0 xxxxxxx</td>
<td>T1/T2/T3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10: 01 00000000</td>
<td>Timing advance value: 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11: 01 00000001</td>
<td>Length of Mobile Allocation: 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12: 0f 00000000</td>
<td>Mobile Allocation ARFCN #4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12: 0f 00000000</td>
<td>Mobile Allocation ARFCN #3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12: 0f 00000000</td>
<td>Mobile Allocation ARFCN #2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12: 0f 00000000</td>
<td>Mobile Allocation ARFCN #1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HoppingChannel
Mobile Allocation Index Offset (MAIO) 2
Hopping Seq. Number: 43
Mobile Allocation ARFCN #4
Mobile Allocation ARFCN #3
Mobile Allocation ARFCN #2
Mobile Allocation ARFCN #1
Message Sequence

Paging

BTS
Message Sequence

Paging

Request channel

Assign channel

exchange info

BTS
Message Sequence

1. Paging
2. Request channel
3. Assign channel
4. Exchange info
5. Start Ciphering
Message Sequence

- Paging
- Request channel
- Assign channel
- Exchange info
- Start Ciphering
- Ciphering started
Message Sequence

Paging
Request channel
Assign channel
Exchange info
Start Ciphering
Ciphering started
Exchange info
Message Sequence

Paging
Request channel
Assign channel
exchange info
Start Ciphering
Ciphering started
exchange info
Ass. speech chn.
Conversation
Hopping Problem
Conclusion

- Still hard to eavesdrop in general
- Other attacks have become feasible
- The GSM system can still use a lot of testing
Questions
A single sub-frequency
A single sub-frequency

$$200\text{KHz}$$
Time division
Time division
Bursts

4.615ms

0 1 2 3 4 5 6 7

576.9μs
Logical channels

\[ \text{TS0 TS1 TS2 TS3 TS4 TS5 TS6 TS7 TS0 TS1 TS2 TS3 TS4 TS5 TS6 TS7} \]