Locating Mobile Phones using Signalling System #7

Tobias Engel <tobias@ccc.de>
twitter: @2b_as
What is Signalling System #7?

- protocol suite used by most telecommunications operators throughout the world to talk to each other
- standardized in ITU-T Q.700 series
- when it was designed, there were only few telecoms operators, and they were either state controlled or really big corporations
- trusted each other, so no authentication built in
- today, everybody can be an operator (e.g. VoIP), so SS7 access is easier to get
Mobile Application Part (MAP)

- part of SS7 that specifies additional signalling that is required for mobile phones to work (roaming, SMS, etc.)
- standardized in 3GPP TS 29.002
- in order for two network operators to talk MAP to each other they usually need a roaming agreement
Structure of a GSM network (key elements)

**Base Station Subsystem (BSS)**

- Air (Um)
- BTS
- BSC
- PCU

**Network SubSystem (NSS)**

- PSTN
- HLR/AUC/EIR
- SS7 Network

**Interface Names**

- Base Station Subsystem: the radio stuff (cell towers etc.)
- Mobile Switching Center: a switch that routes calls and messages from and to your phone and other switches
- Visitor Location Register: a database close to your current location that has a copy of your subscription data from the HLR
- Home Location Register: the database that knows your phonenumber and which network you are currently visiting
What does the network know about your location?

- the location of the cell tower is also a pretty good approximation of your location
- but that information is only known to the network you are currently logged into
- restricted to technical operation of the network - exceptions:
  - "Locate my phone" services
    - have to assure the operator that they have the consent of the phone's owner
    - doesn't work anymore as soon as you are logged into a network that is not your home network
  - Law enforcement
    - have to call the operator of the network you are currently logged into (not your home network operator)
Can somebody with SS7/MAP access find out your location?

- services that can be initiated to your phone number from almost anywhere in the global SS7 network are
  - voice calls
  - short messages

Let's see if these services give any indication of your location...
Locating mobile phones using SS7

Call setup

Home network (HPLMN)
- Gateway switch (GMSC)
- Home DB (HLR)

Visited network (VPLMN)
- Switch (MSC)
- Radio interface (BSS)
- Visitor DB (VLR)

Call setup message (IAM)
- MAP_SEND_ROUTING_INFORMATION
- MAP_PROVIDE_ROAMING_NUMBER
- MAP_PROVIDE_ROAMING_NUMBER Ack
- MAP_SEND_ROUTING_INFORMATION Ack

Call setup (SETUP)
Sending a short message

Locating mobile phones using SS7
Sending a short message

Home network (HPLMN)
- Home DB (HLR)
- MAP_SEND_ROUTING_INFO_FOR_SM
- MAP_SEND_ROUTING_INFO_FOR_SM Ack
- MAP_MT_FORWARD_SHORT_MESSAGE

Visited network (VPLMN)
- Switch (MSC)
- Visitor DB (VLR)
- Radio interface (BSS)
- Message transfer
MAP-SEND-ROUTING-INFO-FOR-SM (3GPP TS 29.002)

- no correlation between requesting routing info for a message and actually sending a message
- SMS are sent directly from the SMSC of the sender to the MSC that you are currently using

- successful request returns:
  - your IMSI ("real" phone number)
  - global title of MSC you are using
  - user error (e.g. "Absent subscriber" == your phone is off)
Mobile Switching Center (MSC)

- handles calls and SMS
- can only handle a certain amount of calls, so in big cities there might be more than one MSC for each network, while in the countryside one MSC might serve a really large area
- global title of the MSC tells us which country you are currently in, because it starts with the country code
- maybe also the network, if mobile networks in that country can be identified by their area code
- other than that: numbering is operator internal

... but that doesn't mean that we cannot get further information from the number by looking at it long enough
## MSC global title (examples)

<table>
<thead>
<tr>
<th>City</th>
<th>T-Mobile Germany</th>
<th>Vodafone Germany</th>
</tr>
</thead>
<tbody>
<tr>
<td>Berlin</td>
<td>+491710360000</td>
<td>+491720012097</td>
</tr>
<tr>
<td>Hamburg</td>
<td>+491710400000</td>
<td>+491720022097</td>
</tr>
<tr>
<td>Frankfurt</td>
<td>+491710650000</td>
<td>+491720061097</td>
</tr>
<tr>
<td>Stuttgart</td>
<td>+491710700000</td>
<td>+491720076097</td>
</tr>
<tr>
<td>München</td>
<td>+491710870000</td>
<td>+491720082097</td>
</tr>
</tbody>
</table>
### MSC global title (examples)

<table>
<thead>
<tr>
<th>City</th>
<th>T-Mobile Germany</th>
<th>Vodafone Germany</th>
</tr>
</thead>
<tbody>
<tr>
<td>Berlin</td>
<td>+491710360000</td>
<td>+491720012097</td>
</tr>
<tr>
<td>Hamburg</td>
<td>+491710400000</td>
<td>+491720022097</td>
</tr>
<tr>
<td>Frankfurt</td>
<td>+491710650000</td>
<td>+491720061097</td>
</tr>
<tr>
<td>Stuttgart</td>
<td>+491710700000</td>
<td>+491720076097</td>
</tr>
<tr>
<td>München</td>
<td>+491710870000</td>
<td>+491720082097</td>
</tr>
</tbody>
</table>

- **First digit of area code**
- **First digit of ZIP code**
Automated approach to narrow down the area an MSC is serving (1/2)

• Rop had a great idea: if we have a lot of mobile phone numbers and already know their location, we could query the network for the current MSC of these numbers, thus creating a MSC ↔ geolocation mapping

• thanks to erdgeist, we have a decoded copy of the "Das Telefonbuch" CD

• sent tens of thousands of MAP_SEND_ROUTING_INFO_FOR_SM requests for numbers from the phonebook
  • requests were done at night, when most people are at home
  • removed the obvious errors
Locating mobile phones using SS7

+491710360000
+49 17 200 22097
+491760000375
Automated approach to narrow down the area an MSC is serving (2/2)

- big thanks to itsme, who created such a mapping for the Netherlands

- other countries also possible if there are phone books available
"No one I know is a network operator - so I can be pretty sure that no one who would care finds out my location, right?"

- wrong: there are several companies offering a lookup service where you send them an MSISDN, they perform a MAP-SEND-ROUTING-INFO-FOR-SM request and send the IMSI and MSC they receive from the HLR back to you

- cost per request is in the low single euro cent area
What is the business case for selling this service?

- Evil_Spammer wants to send spam SMS without paying
- he has SS7 access, and can also send MAP requests, but of course he has no roaming agreements with any other operators, so they don't answer his requests
- but: sending a message via MAP_MT_FORWARD_SHORT_MESSAGE does not even require an answer!
- Evil_Spammer just needs to know, to which MSC the message should be sent, so he uses one of these services...
- then he sets the sender address of the SMS request to that of another networks short message center
- the receiving network bills the SMS to that other network → free spam SMS!
I don't want to be located - what can I do? (1/2)

• SMS "home routing" (3GPP TR 23.840) will fix the problem
  • all messages to your phone are routed to an SMS router in your home network
  • that router will then deliver the message to your phone
  • MAP-SEND-ROUTING-INFO-FOR-SM only returns the ISDN number of the SMS router
  • instead of the IMSI, a random "correlation id" will be returned
  • operators will implement this to
    - prevent fraud
    - enable "VAS"
    - enable "lawful interception" of SMS sent to you when you are in another country
SMS "home routing" (3GPP TR 23.840)
I don't want to be located - what can I do? (2/2)

- until home routing is in use:
  - some networks offer multiple SIMs for one phone number and use an SMS router to decide which SIM will receive the SMS (e.g. o2 Germany)
  - let your operator block incoming SMS for your phone number
  - switch your phone off
What's next: Optimal routeing

- Specified in 3GPP TS 23.079
- makes it possible to route calls directly to the network you are currently logged into

- this can only work if the entity that sets up the call has a way of finding out, which MSC you are currently using...

- OR is currently not widely in use
- charging issues have to be worked out
Call setup with Optimal Routeing

SS7

Home network (HPLMN)

Visisted network (VPLMN)

Switch (MSC)

Visitor DB (VLR)

Radio interface (BSS)

MAP_SEND_ROUTING_INFORMATION

MAP_PROVIDE_ROAMING_NUMBER

MAP_PROVIDE_ROAMING_NUMBER Ack

IAM

MAP_SEND_ROUTING_INFORMATION Ack

SETUP

Locating mobile phones using SS7
Questions?
References

- Signalling System #7, ITU-T Q.700 series: http://www.itu.int/rec/T-REC-Q/e
- Reverse-Engineering für Ortsfremde, Datenschleuder #77 (Seite 26): http://ds.ccc.de/pdfs/ds077.pdf
- Leichtes Spiel mit symboltables, Datenschleuder #86 (Seite 63): http://chaosradio.ccc.de/media/ds/ds086.pdf
- Study into routeing of MT-SMs via the HPLMN, 3GPP TR 23.840: http://www.3gpp.org/ftp/Specs/archive/23_series/23.840/