IMSI Pseudonymization - Feature #4404

Research: Make sure that we can silently detach the IMSI

02/19/2020 10:34 AM - osmith

Status:	Stalled	**Start date:**	02/19/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	70%
Category:			
Target version:			
Spec Reference:			

Description

laforge wrote:

> neels wrote:
>
> > The usefulness of the project seems to pivot on the visibility of the IMSI Detach.
> > If we can't omit the IMSI Detach message, then we either introduce an interruption in network service,
> > or we make it easy to correlate old and new IMSIs by time correlation of Detach and Attach.
>
> I doublt IMSI DETACH is used much in real-world networks these days as it is unauthenticated
> and hence subject to spoofing.

Here's a checklist to prove whether this works or not.

Related issues:

Related to IMSI Pseudonymization - Feature #4400: Approach C: HLR decides and...	**Resolved**	**02/17/2020**
Related to IMSI Pseudonymization - Bug #4480: Applet/OsmoMSC: fix or workarou...	**New**	**04/01/2020**

History

#1 - 02/19/2020 10:46 AM - osmith

- Checklist item changed from Extend the SIM applet to set a timer and perform a new location update after changing the IMSI to Extend the SIM applet to perform a new location update after changing the IMSI
Checklist item [ ] Get Hello World SIM applet running added

#2 - 02/19/2020 12:55 PM - osmith

- Checklist item deleted (Create a SIM applet, which changes the IMSI to a hardcoded new value)
Checklist item deleted (Extend the SIM applet to perform a new location update after changing the IMSI)
Checklist item deleted (Check whether an IMSI detach is sent by the SIM or not)
Checklist item deleted (If an IMSI detach is sent, try to silence it with the SIM applet)
Checklist item deleted (Get Hello World SIM applet running)

- Subject changed from Proof of concept for silent IMSI detach to Make sure that we can silently detach the IMSI

laforge pointed out, that we can just look at SI/LU accept of widespread networks:

> Wouldn't it simply be a test to register to the
> three German networks with a respective operator SIM card and check if switching the
> phone off caues an IMSI DETACH? Or, actually, it would probably be sufficient to look
> at the SI (or the LU ACCEPT?) where the network indicates if IMSI DETACH procedure shall
> be used or not. Any of the above should be possible with OsmocomBB.

#3 - 02/19/2020 02:32 PM - neels

If there is a switch to tell the MS to do silent IMSI Detach, then it should be sufficient to set it.
Spent some time looking, but couldn't find any such SI switch in TS 44.018, nor in the LU messages in TS 24.008.
laforge Am I missing something?

#4 - 02/19/2020 06:21 PM - laforge

On Wed, Feb 19, 2020 at 02:32:02PM +0000, redmine@lists.osmocom.org wrote:

> If there is a switch to tell the MS to do silent IMSI Detach, then it should be sufficient to set it.

It is rather to the contrary: The network tells the MS whether it should perform IMSI DETACH or not. So the flag **enables** it.

```
TS 04.08 Section 4.3.4 IMSI detach procedure

The IMSI detach procedure may be invoked by a mobile station if the
mobile station is deactivated or if the Subscriber Identity Module (see
3GPP TS 02.17) is detached from the mobile station. A flag (ATT)
broadcast in the SYSTEM INFORMATION TYPE 3 message on the BCCH is used
by the network to indicate whether the detach procedure is required.
```

We've had support for setting this flag via the vty since openbsc commit
2ee7ecddeb423dd8b2be984be58c5aee3b359a2f in 2012:

channel-description attach

The naming is a bit weird, and I think the help/reference may be
outright wrong.

#5 - 02/20/2020 01:55 PM - neels

Ah, I did find that, but interpreted it differently:

```
ATT, Attach-detach allowed (octet 2)
Bit
7
0 MSs in the cell are not allowed to apply IMSI attach and detach procedure.
1 MSs in the cell shall apply IMSI attach and detach procedure.
```

It sounds like it completely disallows attaching to the cell, I thought maybe it's for some kind of handover contingency cell,
i.e. not allowing "Location Update (IMSI Attach)" in the first place. Giving it a try...

Next question is whether a similar flag exists for UTRAN
(for us in particular, we probably need to look at femto cells' dmi config)

#6 - 02/20/2020 04:10 PM - neels

- File trace_filtered.pcapng added

I just tested setting ATT=0 in SI3 Channel Description via

osmo-bsc.cfg

```
network
 bts N
  channel-description attach 0
```

With ATT=0, indeed the IMSI Detach Indication is omitted, but the phone also does not send Location Updating (IMSI Attach) either, anymore.

- So, a phone that is switched on does only scan for a PLMN it already knows, shows to the user that it is attached, but never registers. The network has no clue that the phone is available.
  In the case of OsmoMSC, we would also not Page for this subscriber.
- When the phone first requests anything, e.g. *#100#, it gets rejected by the MSC (CM Service Reject, cause "IMSI unknown in VLR").
- The phone then does a Location Updating (Type "Normal").
- After that, a CM Service is accepted and Paging would happen.

So, we not only lose IMSI Detach, but also IMSI Attach, as the specs indicate.

It seems that a SIM that modifies its IMSI must then initiate some sort of CM Service Request so that it gets attached to the MSC.
I wonder whether a phone that moves to a different cell still does a Location Updating? Probably yes?
Then, maybe maybe, if a base band gets a new IMSI, does it consider being moved to a new cell and sends a Location Updating? We need to test.

I wonder how commercial networks solve this, given they have ATT=0 set. Do they always consider all of their IMSIs attached at the last seen MSC?
Probably an MSC (that has lost its VLR state)

- implicitly does an Update Location procedure towards the HLR as soon as a CM Service Request arrives?
- always Pages MSISDNs even if they are not attached?

So ... we can switch off IMSI Attach+Detach and run a Proof-of-Concept that a SIM can change its IMSI.
Then, to not remain unreachable after an IMSI change, the SIM could run an arbitrary CM Service Request towards the CN to enforce a LU.
Otherwise we could enable OsmoMSC to implicitly attach subscribers and always Page everyone, somehow.

Todo:

- ATT=0 on UTRAN?
- How does a SIM/baseband behave when its IMSI is changed?

#7 - 02/20/2020 04:22 PM - neels

With ATT=0, LU (Periodic) still happen as usual.

#8 - 02/21/2020 02:35 PM - osmith

- Related to Feature #4400: Approach C: HLR decides and sends the entire next pseudo IMSI to SIM added

#9 - 02/21/2020 02:48 PM - osmith

> How does a SIM/baseband behave when its IMSI is changed?

Let's add a menu entry that changes the IMSI to check this: #4412

#10 - 03/27/2020 04:07 PM - osmith

> How does a SIM/baseband behave when its IMSI is changed?

When I checked last month on a feature phone, changing the IMSI would display a waiting screen for ~10 seconds (saying something like the SIM is being updated). I wanted to reproduce it now, measure the time and analyze a bit more how it behaves in wireshark, also reproduce what Neels wrote about ATT=0. But for some reason MS did not attach to the BTS at all, I'll debug this next week...

Neels also told me last month, that on a smart phone there would be an indicator for around the same length of time, that says that the SIM is being updated.

Anyhow, the waiting delay is not great for a usability perspective. But if we only change the IMSI rarely, say every hour or every few hours, it seems like a good trade-off between increased privacy due to IMSI pseudonymization and a little decreased usability.

> ATT=0 on UTRAN?

I've spent some time on researching this, but could not a spec reference like it was found for GERAN. Maybe laforge knows this without looking it up, or can provide a pointer to where to look?

#11 - 03/27/2020 04:08 PM - osmith

- Status changed from New to In Progress

- % Done changed from 0 to 50

#12 - 03/31/2020 10:32 AM - osmith

- Checklist item [ ] Register to the three German networks with a respective operator SIM card and check if switching the phone off caues an IMSI DETACH (or check for ATT flag) added
Checklist item [x] How does a SIM/baseband behave when its IMSI is changed? added
Checklist item [ ] ATT=0 on UTRAN? added

- % Done changed from 50 to 70

osmith wrote:

> > How does a SIM/baseband behave when its IMSI is changed?
>
> When I checked last month on a feature phone, changing the IMSI would display a waiting screen for ~10 seconds (saying something like the SIM is being updated). I wanted to reproduce it now, measure the time and analyze a bit more how it behaves in wireshark, also reproduce what

> Neels wrote about ATT=0. But for some reason MS did not attach to the BTS at all, I'll debug this next week...

After inserting the SIM with the SIM applet into a smartphone, it also would not register at first. But after waiting a few minutes, it worked again and now the SIM is working normally in both phones (smartphone and feature phone).

The feature phone displays a waiting screen for 16 to 17 seconds (!) (measured three times with a stop clock), during which the phone can not be used. The smartphone only for ~5 seconds and the UI is not blocked (-> definitively less annoying). For real world usage, it would probably be useful to let the user configure the desired minimum rate at which a new pseudo IMSI should be provisioned. People with smartphones where it is not so annoying could set it to a higher rate than people with a feature phone that becomes unusable as the IMSI changes, and people with a high requirement for privacy could set it to a high rate too (no matter which hardware they use). I have added a related note to the README.

Neels wrote:

- When the phone first requests anything, e.g. *#100#, it gets rejected by the MSC (CM Service Reject, cause "IMSI unknown in VLR").
- The phone then does a Location Updating (Type "Normal").
- After that, a CM Service is accepted and Paging would happen.

I was able to reproduce this (using ATT=0).

#13 - 04/01/2020 07:31 AM - osmith

- Status changed from In Progress to Stalled

laforge will send us OsmocomBB phones to test for ATT=0 in German real-world networks.

#14 - 04/01/2020 08:29 AM - osmith

- Related to Bug #4480: Applet/OsmoMSC: fix or workaround for OsmoMSC only paging attached MS added

#15 - 04/15/2020 10:06 AM - osmith

- Subject changed from Make sure that we can silently detach the IMSI to Research: Make sure that we can silently detach the IMSI

Files

trace_filtered.pcapng	814 KB	02/20/2020	neels