



This is your **last** free member-only story this month. [Sign up for Medium and get an extra one](#)

What is AT&T doing at 1111340002?

Welcome to the magical world of proactive SIMs.

 David Allen Burgess [Follow](#) 
Jul 3, 2021 · 8 min read ★



An AT&T SIM from 2015

From time to time, an attorney will request cellphone activity records from a mobile operator, and those records will show some text messages to and from strange numbers. There is a good chance that the person who uses the phone never sent or saw these messages. And if this happens in the middle of a legal case where cellphone activity is an issue, the resulting confusion can be a source of doubt and error.

In the Spring of 2021, an attorney contacted me about a mysterious SMS to 1111340002, at the center of a wrongful death lawsuit, with allegations of distracted driving. Here is what I found...

TL; DR: The driver's AT&T SIM sent an SMS to 1111340002 to report that the phone had installed an automatic software update. The SMS event had nothing to do with any specific actions by the driver. It took some lab work and a subpoena to AT&T to sort this out.

The SIM

The SIM used for this investigation is the one in the photo. It was issued by AT&T, probably in 2015.

The Tools

The tools used for this investigation are well known in the mobile network security research community, and all based on open source designs that can be verified by other parties:

- YateBTS, based on [OpenBTS](#), used to simulate a cellular network.
- [SimTrace2](#), a tool for monitoring communication between the SIM and the phone.
- [Wireshark](#), a protocol analyzer that can decode the outputs of YateBTS and SimTrace2.

I also used a variety of phones, from Nokia, Samsung, and others.

With this test bench, I could simulate a cellular network and then record examples of the phones sending the SMS to 1111340002.

And, for the record, the actual test bench was located in Romania. This was convenient because it meant that I never had the risk of the SIM contacting the real AT&T network and getting disabled by AT&T, or the risk of handsets in the room accidentally trying to attach to my fake AT&T cell site.

The Destination

Summary: Where is this message going? The destination is a special server somewhere inside AT&T.

Any outgoing SMS from a phone has two destination numbers (“addresses”):

- There is the transport layer (“TP”) destination address, the address of the final recipient, which in this case is 1111340002. (Normally, this is the number that the user specifies.)
- There is the relay layer (“RP”) destination address, the address of the SMSC to use for outgoing routing, which in this case is +14047259800. (Normally, this number is supplied by the SIM.)

The TP destination number 1111340002 does not fit into any public network numbering plan. It must be a private address inside AT&T. This number does not exist in the public network. You cannot call it or text in through normal means. For a message to get delivered to that private address, it must go to a particular AT&T SMSC that knows how to route it.

The RP destination number, +14047259800, is a normal-looking US number, what a telecom engineer would call an “NANP E.164”. A Google search turns up documents showing that this number is associated with an AT&T “service control point” (a sort of server) that was made by Sun Microsystems. This is most likely a Sun Solaris server running an Oracle SMSC package, physically located in Atlanta, GA. Interestingly, this is not the SMSC number that AT&T uses for normal texting (+13123149810). This is a special SMSC that is used for special applications.





Midtown Atlanta. See the AT&T building? The tall white one, just to the right of center? These messages are going to one of AT&T’s data centers in the metro-Atlanta area, though not necessarily to this building. There are no publicly-available photos of the data centers, so we have this building as a symbol of AT&T’s massive corporate presence in the Atlanta area, mostly as the legacy of Southern Bell. Photo by [Kyle Sudu](#) on [Unsplash](#).

The Content

Summary: What is in the message? The message reports information about the SIM, about the phone, *and about the phone that the SIM was previously installed in*, and some other stuff that I have not figured out yet.

The SMS payload is indicated as being raw binary, not normal SMS text. It has a regular structure, using the same type-length-value (“TLV”) formatting that is used in many telecom protocols. Here is an example of the actual message content, taken with YateBTS and Wireshark:

Reassembled LAPDm frame, SMS payload in bold:

0000 : 19 01 9b 00 01 00 07 91 41 40 27 95 08 f0 8f 15A@’.....

0010 : 01 0a 81 11 11 43 00 20 00 f4 ff 82 ee **01 50 22**C.P”

0020 : **09 08 39 01 14 20 95 64 66 89 23 09 33 25 76 03** ..9.. .df.#.3%v.

0030 : **08 91 23 76 f8 24 09 33 25 88 16 90 55 35 01 f6** ..#v.\$3%...U5..

0040 : 25 20 ff ff ff ff 7f 9f 00 df ff 00 00 1f e2 08 %

0050 : 11 06 c3 c0 00 00 00 00 40 00 51 00 00 00 00 18@.Q.....

0060 : 00 00 26 10 01 01 01 01 00 00 03 01 00 00 00 00 ..&.....

0070 : 00 00 00 00 20 0a 98 10 14 40 72 52 49 66 96 98@rRlf..

0080 : 21 07 13 00 14 03 e2 03 e2 27 10 00 00 00 00 00 !.....'.....

0090 : 00 00 00 00 00 00 00 00 00 00 00 28 01 02(.

Decoding:

- Header 0xEE0150, unknown meaning, but consistent. Possibly encodes the protocol version.
- Field type 0x22, length 9, the IMSI of the SIM
- Field type 0x23, length 9, the IMEISV of the previous phone using this SIM
- Field type 0x24, length 9, the IMEISV of the current phone using this SIM
- Field type 0x25, length 32, the terminal profile of the current phone
- Field type 0x26, length 16, unknown purpose
- Field type 0x20, length 10, the ICCID of the SIM
- Field type 0x21, length 7, the location area in the current serving network
- Field type 0x27, length 16, unknown purpose, all zero
- Field type 0x28, length 1, unknown purpose

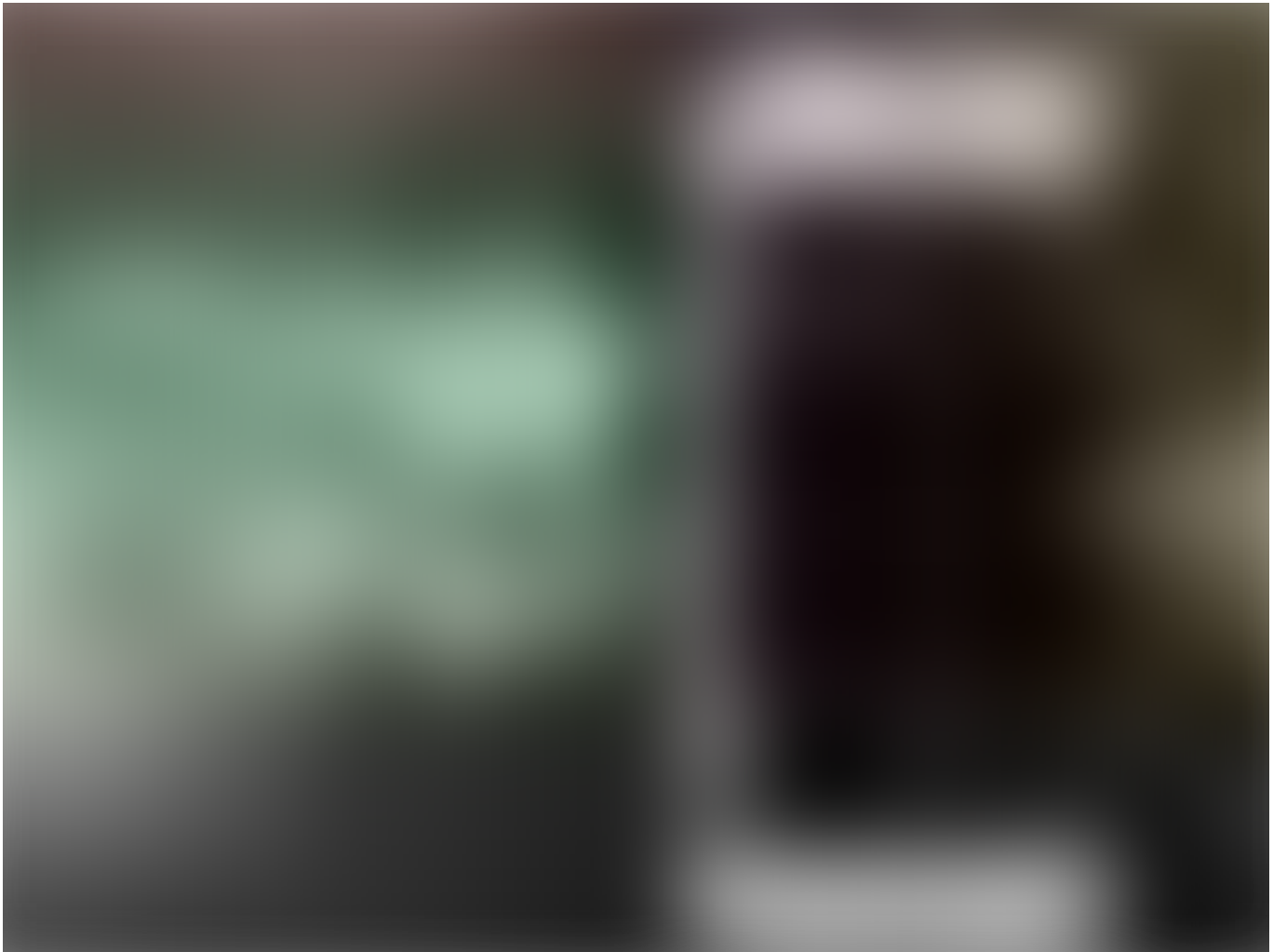
The Source

Summary: What is sending this message? The SIM.

The fact that the message carries information about the previous phone that used the SIM is a strong hint that the SIM itself is sending the message, because only the SIM would “remember” this information as it moves from one phone to another.

SIMs can send SMS on their own using a feature called “proactive MO-SMS”.

To verify that the SIM was the source, I used the SIMTrace2 SIM tracing tool. The tracing tool connects to the phone’s SIM tray with a special flat cable. The SIM plugs into the tracing tool. Now the tracing tool sits between the phone and the SIM, and it can record the commands and responses exchanged between them. And, sure enough, the tracing tool recorded the SIM using proactive MO-SMS to send this message, just a second or two before the message arrived in the YateBTS cell simulator.



SIMTrace2 tool connected to a test phone, with the SIM installed.

The signaling that is used by the SIM to send this message goes directly between it and the baseband processor. (If that statement does not fully make sense, take a look at [this post on the structure of a smartphone](#).) The application processor, where the user’s SMS messaging app runs, is not “in the loop”. The iOS or Android part of the phone has no way to know what happened. The SIM does not save a copy of the message, either. If

everything is working correctly, there will be no traces left in the SIM or in the phone that this message was sent. The only records of the event will be at AT&T.

The Trigger

Summary: When does the SIM send this message? Whenever the SIM moves to another phone and whenever the firmware is updated in the phone's baseband processor.

The fact that the SIM reports the IMEISV of the phone (and of the previous phone) is a sign that a change of IMEI probably triggers the message. And, sure enough, moving the SIM from one phone to another, exposing the SIM to a new IMEI, does trigger the message. In fact, that is how I learned to trigger the message on demand to do some of the examinations that I describe here.

Judging from AT&T activity records, there are other triggers as well, because the IMEI appears in several places in a typical AT&T activity record, and that IMEI is usually not changing. Just determining these triggers through reverse-engineering may not be possible and is certainly not practical. At this point, a carefully crafted subpoena to AT&T is probably the most efficient way to find the other triggers, if you are in a position to do that. However, examination of the signaling between the SIM and the phone does rule out some causes:

- The triggers are not time-based. There is no clock in the SIM and the SIM never asks the phone for the current time, even though it has many opportunities.
- The triggers are not based on user activity. There is no signaling between the SIM and the phone that would indicate user activities that do not explicitly require the SIM. Again, the SIM has opportunities to request information about user activities, but it does not make such requests.
- The triggers are probably not based on mobility. The SIM reports cell tower data, but changes in call tower data do not appear to trigger the message. I ran several experiments to simulate the effects of the phone moving through the network from tower to tower or across location areas, for days at a time, but none of them triggered the message.

After the lab work, deposition of an AT&T employee revealed that the only other trigger is a firmware update of the baseband processor. That is also consistent with the SIM

requesting the IMEISV, since the “SV” part means “software version”, and it is updated every time the baseband processor loads new firmware. In this particular case, the phone had recently downloaded an update that included new baseband firmware. That was almost certainly the trigger for this message.

The Purpose

AT&T says nothing publicly about why their SIMs send these reports, but it seems that they are trying to keep a database of what phones their customers are using, and where. That is obviously useful information for an operator, although it would be nice if they were transparent about it.

And there is other information in the message whose purpose is not yet known.

Conclusion

AT&T is not the only operator to use pro-active SIMs to send automatic SMS back to their network. They are given here only as an example. The point here is that the cellphone literally has a mind of its own, in fact multiple “minds”, including in the SIM. These various minds might not even be talking to each other, and just because a phone did something, that doesn’t mean that user caused it.

[Sim Card](#) [Sms](#) [Cell Phones](#)

[About](#) [Write](#) [Help](#) [Legal](#)

Get the Medium app

