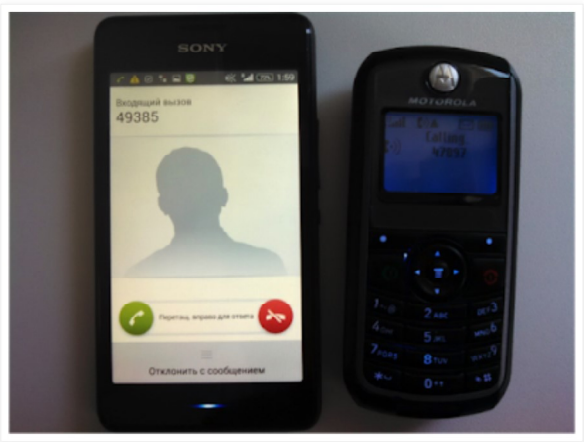
Positive Technologies - learn and secure

October 30, 2015

HackerSIM: Blamestorming



Recently, there have been a lot of articles about a SIM card that has some incredible features. This topic sparked a lively discussion full of skepticism and mind-blowing theories. Let's lift the veil on some technical aspects of this story. Of course, we wouldn't be able to carry out the tests without the SIM card provided by @MagisterLudi.

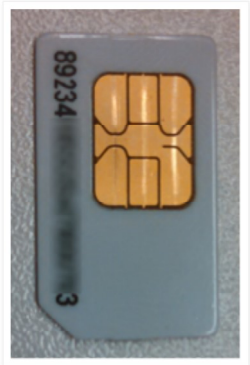
A short resume for those who don't want to read the whole review:

- There is no forced encryption, protection from intercept complexes, connection to a base station with the second strongest signal, IMSI and location hiding.
- There is phone number substitution, voice substitution, and billing.

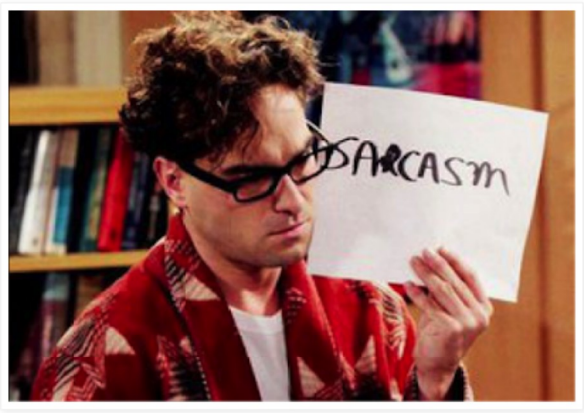
Let's take a closer look at each of these features.

Our first disappointment

There was no Anonymous mask on the SIM card as in one of the articles:



The icon was the whole point, so we decided to stop our research.



Who does it belong to?

What does the ICCID printed on the SIM card tell us?

Country	CSP	ICCID Prefix	IMSI Prefix (MCC + MNC)	Notes
Italy	WorldSIM (Service Provider Name stored on card is 'Global Roaming')	89234	22201	Although technically an Italian SIM, WorldSIM has been sold on British Airways flights and is targeted at UK customers. The card claims to include "Multi IMSI Technology" and offer both a UK and a US mobile number

We insert the SIM card into the phone, and the first things we see are roaming, MTS connection, and the third line that couldn't escape our attention — AY Security. It indicates the owner of the SIM card: http://www.aysecurity.co.uk/aysim.html

- Positive Technologies Official Site
- PT Telecom Attack Discovery
- PT BlackBox Scanner
- OWASP Top 10 Vulnerabilities
- WAF Security Solutions Explained
- Cross-site scripting (XSS) Attacks - The Definitive Guide

Search

Search

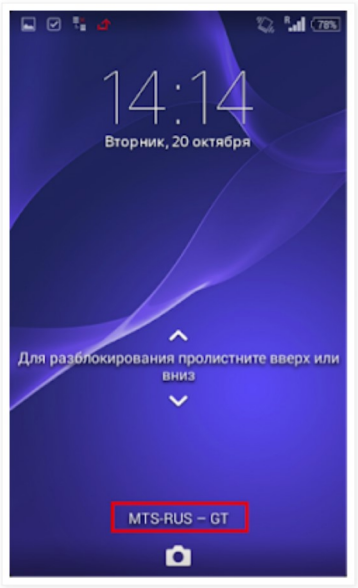
Labels

telecom phdays Best of Positive Research Linux positive technologies PCI DSS audit SQL-Injection Microsoft blackbox positive research

Subscribe

435 readers BY FEEDBURNER

It's a funny thing that our smartphone displays another data (we still have no idea, what "GT" means).



The following "unique" SIM card features are described on the website:

- the caller number substitution,
- forced encryption
- protection against intercept complexes
- voice substitution
- expenses optimization
- real IMSI hiding
- current location hiding
- virtual number

The first and fourth points have been already discussed on Habrahabr, so we will cover the other ones, which are a lot more sophisticated.

Forced encryption

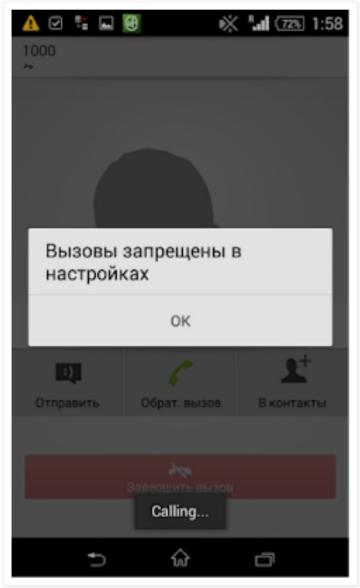
> “This feature prevents your SIM from lowering of encryption level and ignoring the operator or intercept complexes’ commands to switch off the encryption key generation algorithm (A8) stored at a SIM’s module. As a result all your conversations are encoded according to the A5.1. algorithm.”

Initially, the transfer has no encryption, which is enabled by Ciphering Mode Command from the operator. Here's an example from a real network (using HackerSIM):

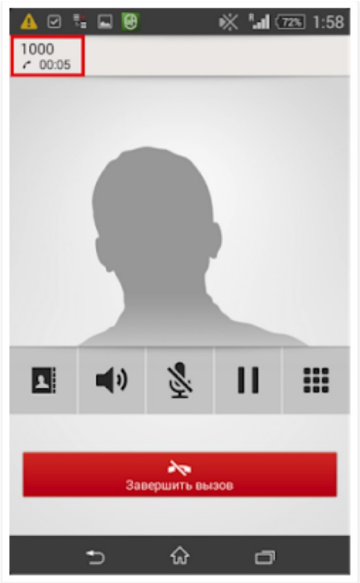
```
Protocol        Length  Info
LAPDm              81 I, N(R)=1, N(S)=1(DTAP) (RR) Ciphering Mode Command
LAPDm              81 S, func=RR, N(R)=2
LAPDm              81 I, N(R)=2, N(S)=1(DTAP) (RR) Ciphering Mode Complete
LAPDm              81 U, func=UI(DTAP) (RR) System Information Type 6
LAPDm              81 U, func=UI
LAPDm              81 I, N(R)=2, N(S)=2(DTAP) (MM) Location Updating Accept
LAPDm              81 S, func=RR, N(R)=3
LAPDm              81 I, N(R)=3, N(S)=2(DTAP) (MM) TMSI Reallocation Complete

⊞ Frame 142: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
⊞ Ethernet II, Src: Vmware_8d:e7:25 (00:0c:29:8d:e7:25), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
⊞ Internet Protocol Version 4, Src: 192.168.183.128 (192.168.183.128), Dst: 192.168.183.1 (192.168.183.1)
⊞ User Datagram Protocol, Src Port: 36086 (36086), Dst Port: 4729 (4729)
⊞ GSM TAP Header, ARFCN: 884 (Downlink), TS: 2, Channel: SDCCH/8 (2)
⊞ Link Access Procedure, Channel Dm (LAPDm)
⊟ GSM A-I/F DTAP - Ciphering Mode Command
  ⊞ Protocol Discriminator: Radio Resources Management messages (6)
    DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
  ⊟ Cipher Mode Setting
      .... ...1 = SC: Start ciphering (1)
      .... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)
  ⊟ Cipher Mode Response
      ...0 .... = CR: IMEISV shall not be included (0)
```

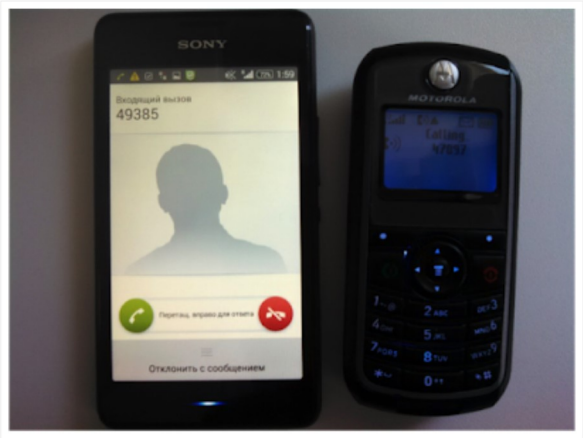
However, it is the same for all the other SIM cards, as all Russian networks usually use encryption. Let's connect to OpenBTS and try to make a phone call to check the restriction of operation without encryption:



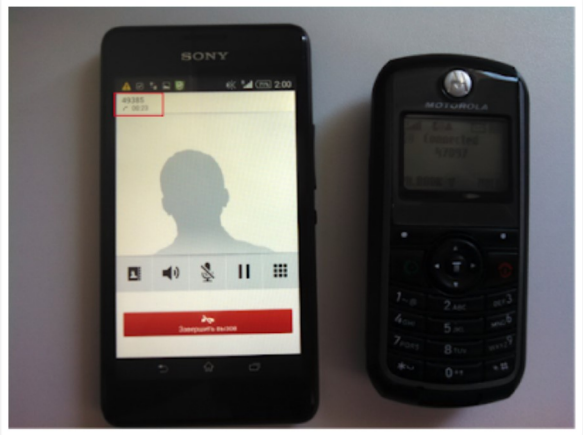
Text on picture: «Outgoing calls forbidden in settings»



The first impression was that the SIM card, indeed, somehow found out that there was no encryption and blocked the call. (It's not true, though; we will touch upon that a bit later. Also, take a look at the "Calling..." message at the bottom of the screen.) However, if you try to make a few phone calls in a row (we made three), the operation will succeed.



There is no problem with terminating phone calls.



It should be mentioned that the vendor claims the restriction applies to voice calls, but SMS messages, both terminating and originating, can be transferred in a fake network without encryption.

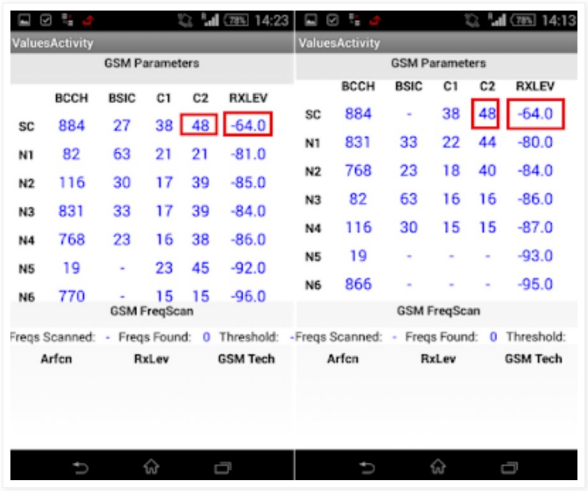
Protection against intercept complexes

> "This function allows you to stay invisible for moving intercept complexes. As the work of such complex is based on the replacement of real base station, it (complex) becomes a priority for all phones which are under the coverage area of real base station. Devices protected by our software ignore stations signals of the highest level."

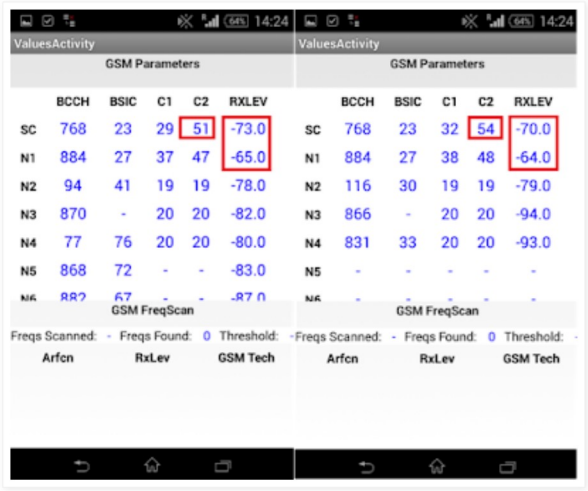
A phone chooses a base station not by the signal level, but by the C2 parameter, which depends on the current signal level, minimum signal strength for the base station, and the base station priority. It's a mistake to think that it can save you from a fake base station. For example, the output power of OpenBTS with an SDR is about 100mW — less than cell phone output (up to 1W), and considerably less than standard base station output. Therefore, high priority — not high power — is required for interception. The fact that a cell phone uses a less powerful base station only means it has a higher priority.

We used the Green Head application [http://green-head.ru/] to measure the power, C1 and C2. The screenshots below show the list of neighbor and serving cells (BCCH — arfcn, SC — serving cell, N1 — neighbor cell 1, etc.).

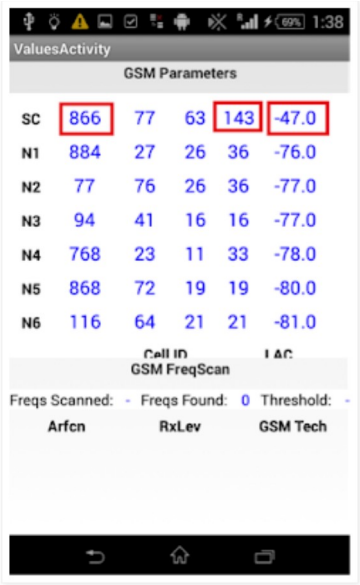
1. HackerSIM on the most powerful and high-priority base station



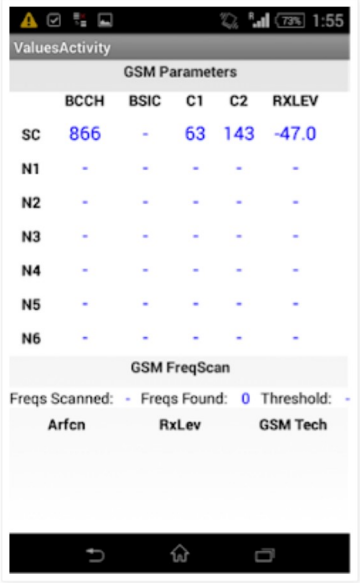
2. HackerSIM on a less powerful base station with the highest priority



3. We turn on the "intercept complex" and... HackerSIM easily connects to it. Or rather, it is the cell phone that connects to it, as SIM cards do not choose cells, and HackerSIM is no exception:



4. After hijacking the phone, the fake network no longer shows the "neighbors", so the phone has no choice other than to stay in the fake network as long as an attacker wants, or until it leaves the coverage area.

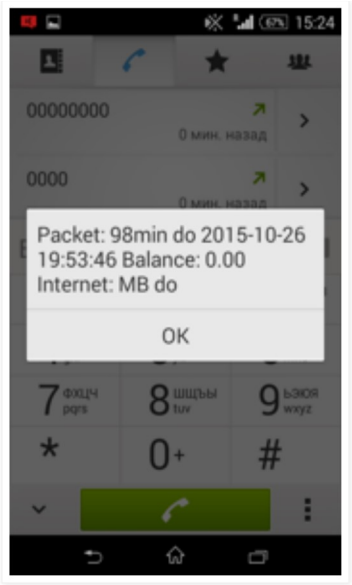


Expenses optimization

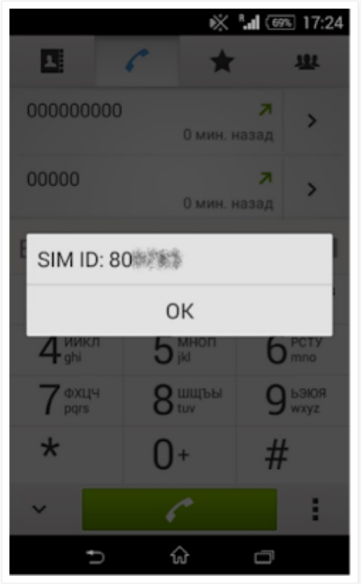
This statement is very creative considering the cost of the SIM card and monthly payments.

Real IMSI hiding/Current location hiding/No billing/Virtual number

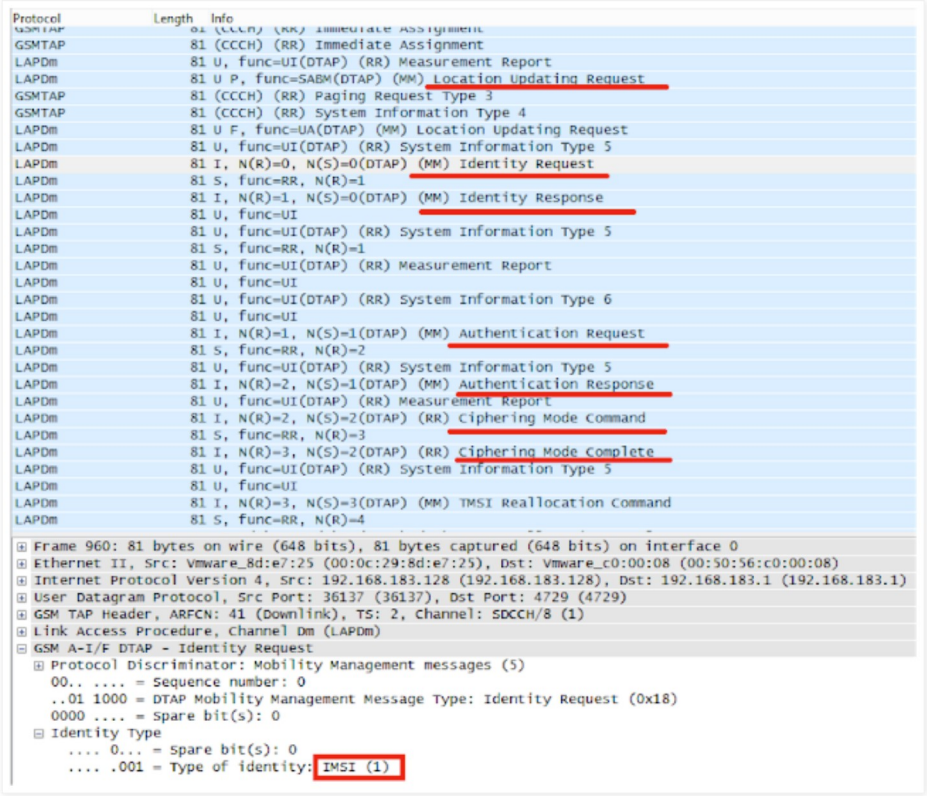
The vendor claims there is no billing, so it's "impossible" to track down a subscriber with HackerSIM. But if there's no billing, who sends this information?

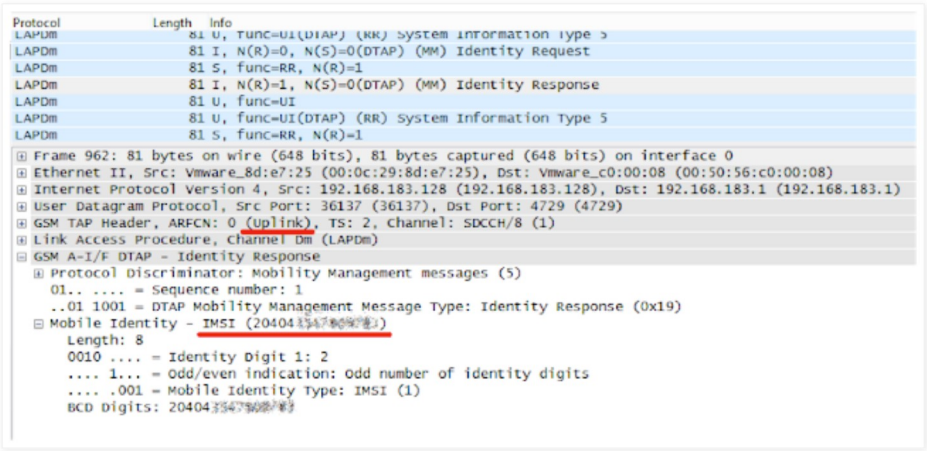


Subscriber location is tracked via SS7 by means of the attacks we've already described [http://www.ptsecurity.com/upload/ptcom/SS7_WP_A4.ENG.0036.01.DEC.28.2014.pdf]. IMSI is enough to determine a subscriber's location. The identifier is usually obtained by the phone number. Our phone doesn't display the number of our HackerSIM, even though we followed the instruction from the vendor's website (there should be DID for making calls):



We can't check if the number is really virtual, as we don't know it. However, you can find out the IMSI through the radio air (e.g., when the phone connects to the network):

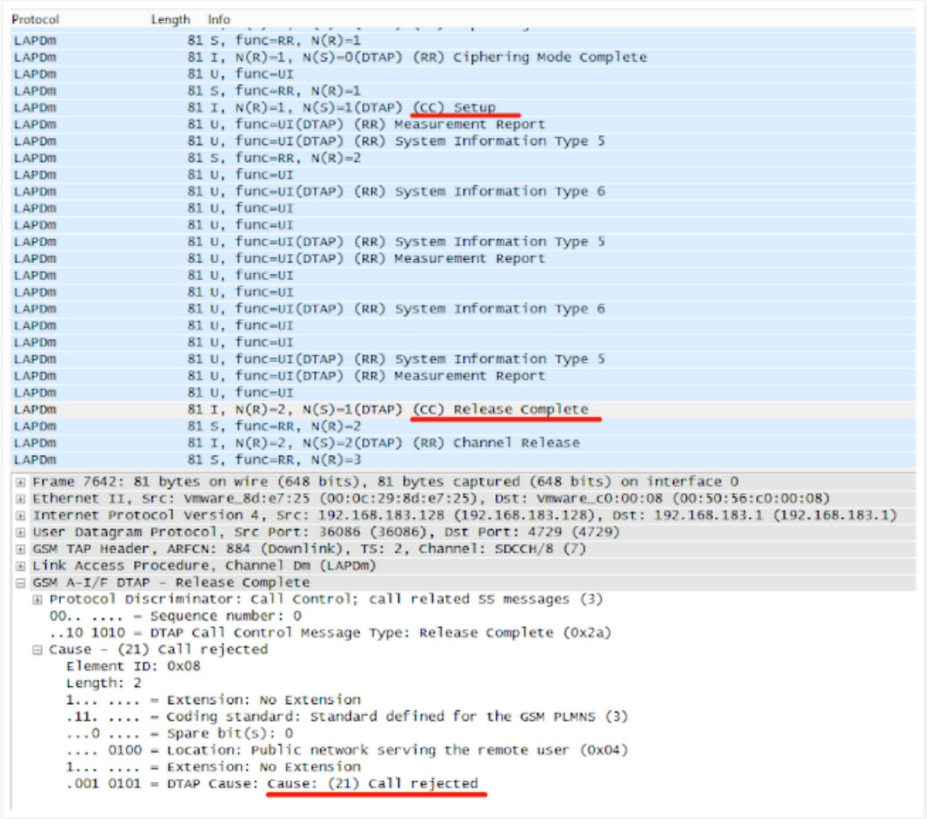




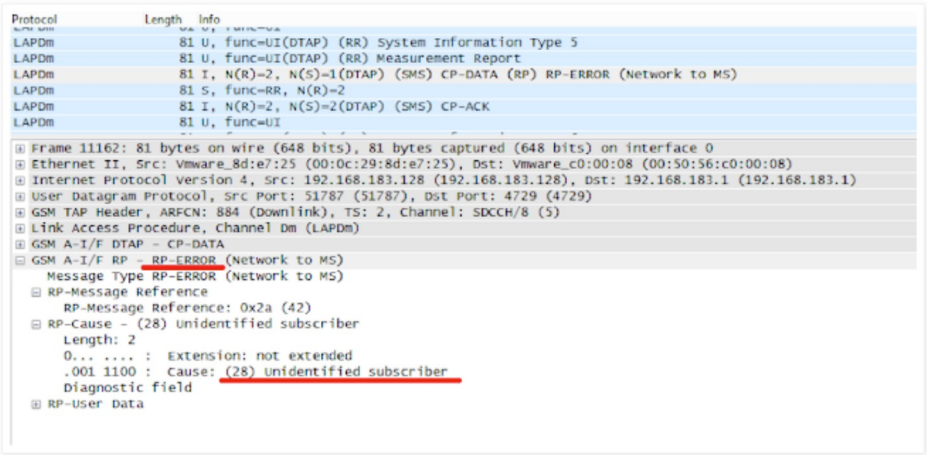
The phone sends Location Update Request, the network asks for the IMSI (Identity Request), and the phone tells its IMSI (Identity Response). After that, the session keys are created (Authentication Request and Authentication Response), and Ciphering Mode Command is sent. In other words, you can intercept the IMSI in the radio network without breaking the encryption, but that's how a cellular network is supposed to work.

There is another question mentioned in HackerSIM' articles that nobody could answer. When a phone is registered in the roaming network, a request is sent to the home network, but after that, all the calls should pass through the visited network. How do all the originating calls pass through the PBX, then? The answer is interesting but simple.

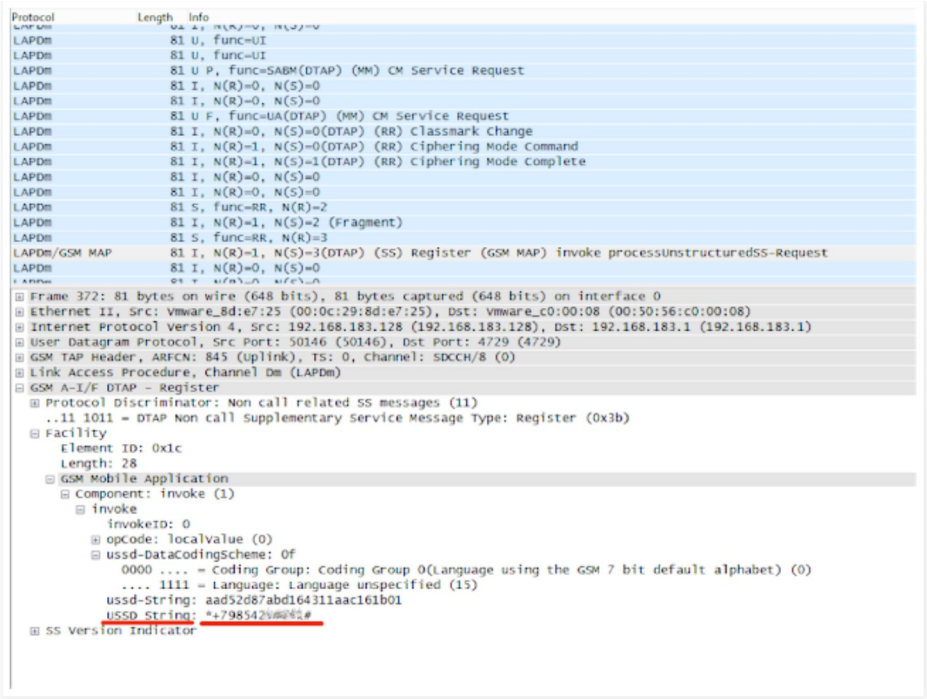
When we used Motorola C118 to originate a call, it was rejected, and nobody called back. The same happened, when we used OsmocomBB Mobile App.



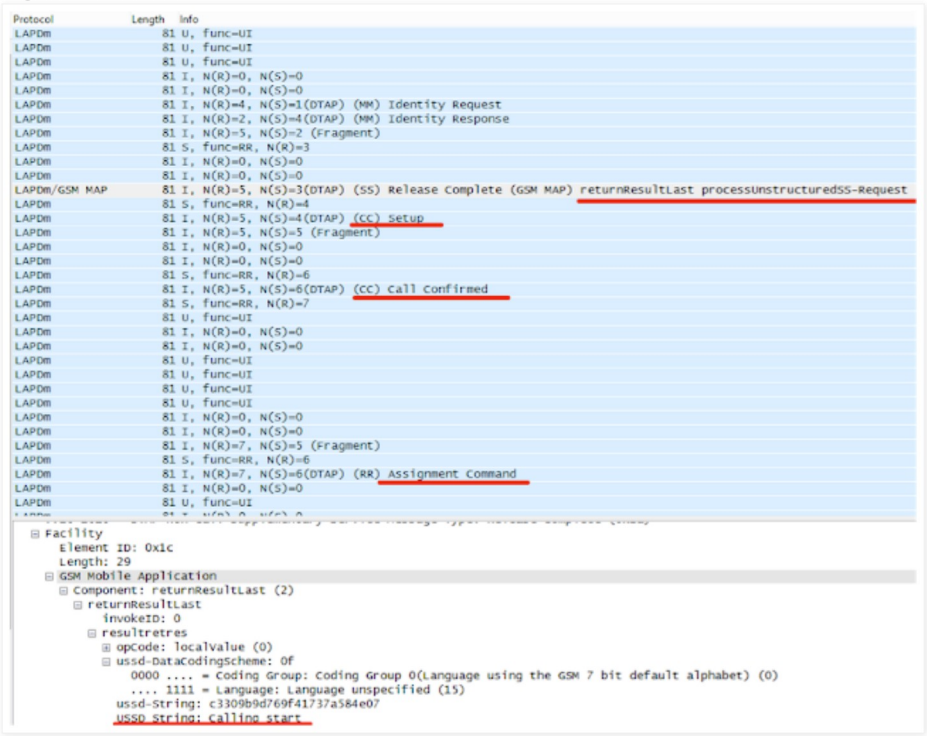
By the way, the reason why SMS messages were rejected is even more peculiar:



Let's get back to why the old Motorola can't originate a call, and the calls from the smartphone get rejected with the PBX calling back. The radio air dump solves the mystery:



When you originate a call, the phone sends a USSD request with the called subscriber number instead of the Setup message. This request wanders around the world for quite a long time and gets to the Netherlands. The home network sends a USSD response with a simple text— Calling start — and after that there's a terminating call with a familiar sequence: Setup, Call Confirmed, Assigned Command.

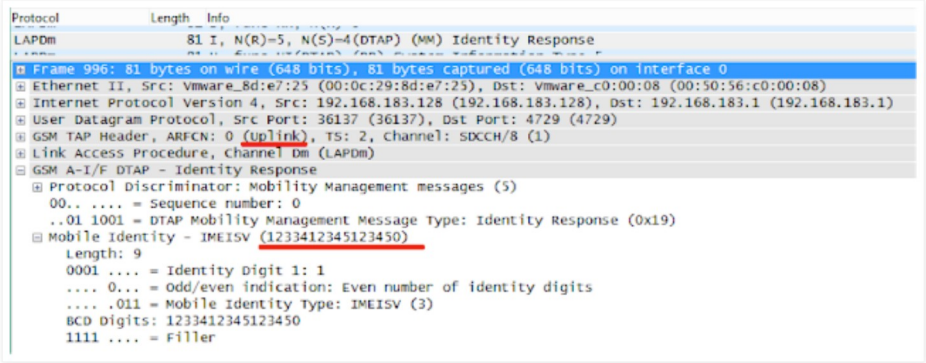


So, the home network disables any originating data transfer of the SIM card apart from USSD requests. The application on the SIM card intercepts the call and instead sends a USSD request containing the called number. After the data is sent to the home network, the application ends the call, displays the message "Calling...", and waits for the USSD response while checking the "encryption".

If the USSD response fails, or there's no Calling start message, it blocks the call (that's what happened in the fake network). However, it seems that the SIM card can't intercept all the calls; if

you overwhelm it with the attempts, the calls become direct.

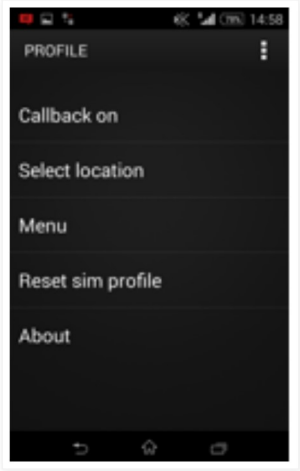
We tried to make a call bypassing the PBX in a real network, but we were "beaten back", because any originating data transfer of HackerSIM is restricted.
The most attentive readers have probably noticed there is an Identity Request message before the USSD response in the previous screenshot. It is used by the network to obtain the IMSI or IMEI from the phone.



We should point out that IMEI is absolutely unnecessary for the cellular network and may be never requested. Hence, someone gathers this data for a reason. If you use HackerSIM, you do not become anonymous: they know — who, where, and when.

Now, knowing the secret of the originating calls, we can use both the old Motorola and OsmocomBB mobile App.

Multi IMSI/Ki
To change the IMSI/Ki pair, you need to use the SIM card menu:



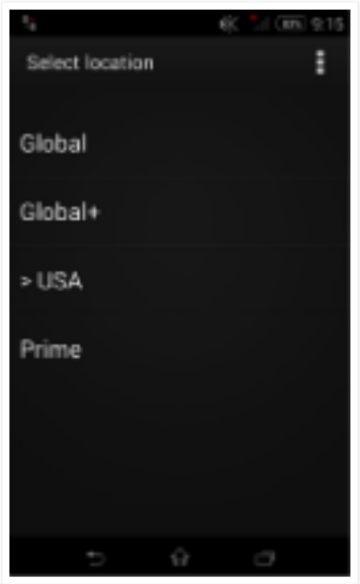
Callback on/off — enables (disables) the SIM card application that replaces originating calls with USSD.

Menu — has nothing except Exit.

Reset sim profile — resets the TMSI and Kc (session key).

About —

Select Location — allows to choose the IMSI/Ki.



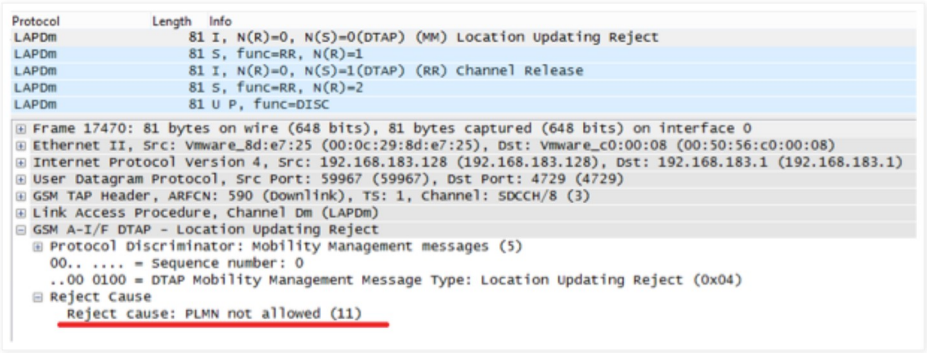
Global — IMSI 22201xxxxxxxxx, belongs to **TIM**, an Italian operator.

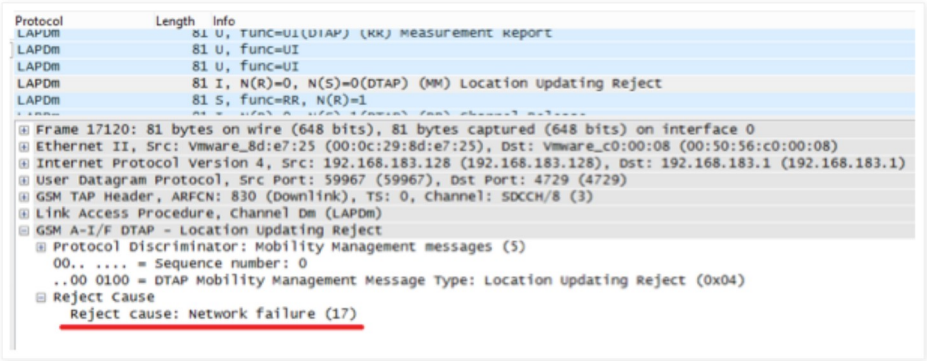
Global+ — IMSI 20404xxxxxxxxx, belongs to **Vodafone Libertel**, a Dutch operator.

USA — IMSI 310630xxxxxxxxx, does not belong to any operator and is used in different Global SIM cards.

Prime — IMSI 23418xxxxxxxxx, belongs to **Cloud9/wire9 Tel**, a British provider.

There are two reasons why all the IMSI numbers, except for **Global+**, are not registered in Russia:





There are some difficulties with the Global+ mode, too.

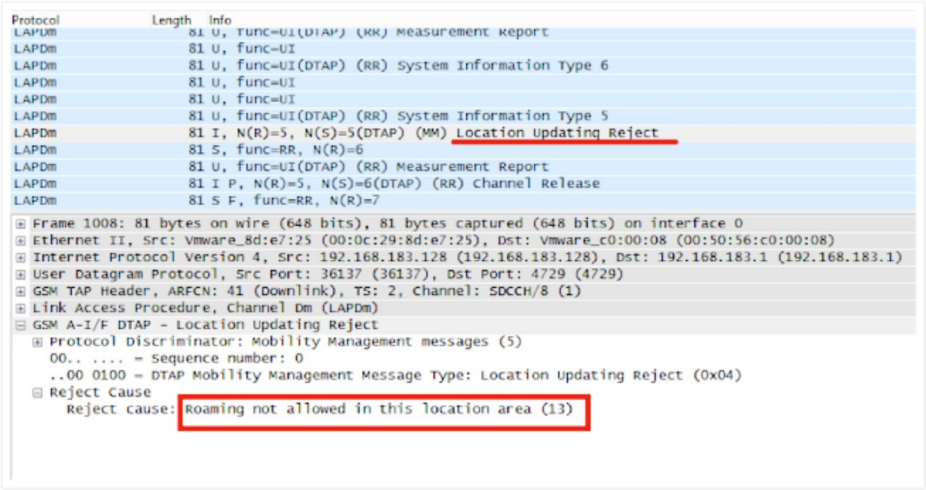
The list of preferred networks (everything will work):

```
List of preferred PLMNs:
        MCC     |MNC
        --------+-------
        234     |15         (Guernsey, Vodafone)
        262     |02         (Germany, Vodafone)
        208     |10         (France, SFR)
        222     |10         (Italy, Vodafone)
        214     |01         (Spain, Vodafone)
        505     |03         (Australia, Vodafone)
        228     |01         (Switzerland, Swisscom)
        206     |01         (Belgium, Proximus)
        404     |20         (India, Vodafone IN)
        404     |11         (India, Vodafone IN)
        404     |27         (India, Vodafone IN)
        404     |05         (India, Vodafone IN)
        404     |46         (India, 46)
        272     |01         (Ireland, Vodafone)
        202     |05         (Greece, Vodafone)
        232     |01         (Austria, A1)
        655     |01         (South Africa, Vodacom)
        286     |02         (Turkey, Vodafone)
        238     |01         (Denmark, TDC)
        268     |01         (Portugal, Vodafone)
        260     |01         (Poland, Plus)
        230     |03         (Czech Republic, Vodafone)
        250     |01         (Russian Federation, MTS)
        216     |70         (Hungary, Vodafone)
        226     |01         (Romania, Vodafone)
```

```
244     |05         (Finland, Elisa)
602     |02         (Egypt, Vodafone)
219     |10         (Croatia, VIPnet)
620     |02         (Ghana, Ghana Telecom Mobile / Vodafone)
255     |01         (Ukraine, MTS)
```

There are no restricted networks, but Beeline or Tele2 will deny your registration, if you try. MegaFon works fine, MTS is preferred (in the SIM card).

That's what happens if you try to connect to Beeline:



Therefore, this SIM card may work in every country in the world, but not in every network.

Resume

The procedure used to originate calls may cause some trouble when searching for the calling subscriber, but only if the PBX is located abroad and not used by intelligence agencies, and service providers don't know or don't want to know anything about these special SIM cards. It's not so hard to track the users of these modules: you will just have to look for slightly different data.

The SIM card itself doesn't have any incredible or hacker features.

Author Positive Research at 11:24 AM

Tags HackerSIM, information security, mobile data bypass, telecom

77 comments:

Unknown October 31, 2015 at 3:49 AM

This comment has been removed by a blog administrator.

Reply

Replies

Unknown February 7, 2016 at 2:24 AM

This comment has been removed by a blog administrator.

Unknown February 16, 2016 at 6:49 PM

This comment has been removed by a blog administrator.

Unknown June 26, 2016 at 9:02 PM

This comment has been removed by a blog administrator.

Reply

Unknown November 8, 2015 at 1:38 PM

This comment has been removed by a blog administrator.

Reply

DevidAA November 9, 2015 at 4:57 AM

This comment has been removed by a blog administrator.

Reply

Unknown November 28, 2015 at 1:18 AM

This comment has been removed by a blog administrator.

Reply

geometrydash December 16, 2015 at 12:33 AM

This comment has been removed by a blog administrator.

Reply

Unknown December 22, 2015 at 8:17 PM

This comment has been removed by a blog administrator.

Reply

Unknown December 28, 2015 at 11:00 AM

This comment has been removed by a blog administrator.

Reply

Unknown December 29, 2015 at 7:05 PM

This comment has been removed by a blog administrator.

Reply

Unknown January 3, 2016 at 6:35 AM

This comment has been removed by a blog administrator.

Reply

Unknown January 3, 2016 at 11:13 PM

This comment has been removed by a blog administrator.

Reply

Unknown January 6, 2016 at 1:05 AM

This comment has been removed by a blog administrator.

Reply

Unknown January 6, 2016 at 11:42 PM

This comment has been removed by a blog administrator.

Reply

Unknown January 7, 2016 at 4:59 AM

This comment has been removed by a blog administrator.

Reply

Unknown January 7, 2016 at 11:02 PM

This comment has been removed by a blog administrator.

Reply

Unknown January 12, 2016 at 1:42 AM

This comment has been removed by a blog administrator.

Reply

Unknown January 12, 2016 at 1:43 AM

This comment has been removed by a blog administrator.

Reply

Unknown January 13, 2016 at 8:49 PM

This comment has been removed by a blog administrator.

Reply

Unknown January 14, 2016 at 7:07 PM

This comment has been removed by a blog administrator.

Reply

Linda Rose January 17, 2016 at 8:49 PM

This comment has been removed by a blog administrator.

Reply

Anita Frank January 23, 2016 at 10:52 AM

This comment has been removed by a blog administrator.

Reply

Anonymous January 24, 2016 at 10:13 PM

This comment has been removed by a blog administrator.

Reply

Unknown January 26, 2016 at 4:27 AM

This comment has been removed by a blog administrator.

Reply

Linda Rose January 28, 2016 at 8:08 PM

This comment has been removed by a blog administrator.

Reply

amin.jamal February 2, 2016 at 2:00 AM

This comment has been removed by a blog administrator.

Reply

Unknown February 6, 2016 at 12:38 AM

This comment has been removed by a blog administrator.

Reply

Unknown February 7, 2016 at 2:22 AM

This comment has been removed by a blog administrator.

Reply

Mrs.Irene Query February 12, 2016 at 7:58 AM

This comment has been removed by a blog administrator.

Reply

Unknown February 15, 2016 at 7:37 AM

This comment has been removed by a blog administrator.

Reply

Mohamed Ali February 24, 2016 at 10:53 PM

This comment has been removed by a blog administrator.

Reply

Unknown February 28, 2016 at 10:36 PM

This comment has been removed by a blog administrator.

Reply

Unknown March 1, 2016 at 1:17 AM

This comment has been removed by a blog administrator.

Reply

Unknown March 6, 2016 at 11:44 PM

This comment has been removed by a blog administrator.

Reply

Unknown March 7, 2016 at 3:18 AM

This comment has been removed by a blog administrator.

Reply

henris March 9, 2016 at 12:56 AM

This comment has been removed by a blog administrator.

Reply

Unknown March 9, 2016 at 2:56 AM

This comment has been removed by a blog administrator.

Reply

alicetaylor March 9, 2016 at 7:27 PM

This comment has been removed by a blog administrator.

Reply

Anonymous April 10, 2016 at 4:56 PM

This comment has been removed by a blog administrator.

Reply

Unknown April 13, 2016 at 6:16 PM

This comment has been removed by a blog administrator.

Reply

Unknown April 17, 2016 at 11:57 PM

This comment has been removed by a blog administrator.

Reply

Unknown April 18, 2016 at 7:49 PM

This comment has been removed by a blog administrator.

Reply

Unknown April 19, 2016 at 9:40 AM

This comment has been removed by a blog administrator.

Reply

Unknown April 24, 2016 at 9:51 PM

This comment has been removed by a blog administrator.

Reply

Unknown April 24, 2016 at 9:52 PM

This comment has been removed by a blog administrator.

Reply

Unknown April 24, 2016 at 9:52 PM

This comment has been removed by a blog administrator.

Reply

Unknown April 24, 2016 at 9:52 PM

This comment has been removed by a blog administrator.

Reply

Unknown April 25, 2016 at 3:17 AM

This comment has been removed by a blog administrator.

Reply

chenzhen April 25, 2016 at 10:29 PM

This comment has been removed by a blog administrator.

Reply

Unknown May 1, 2016 at 11:15 AM

This comment has been removed by a blog administrator.

Reply

Result Saifi May 3, 2016 at 5:02 AM

This comment has been removed by a blog administrator.

Reply

Horace May 5, 2016 at 6:28 AM

This comment has been removed by a blog administrator.

Reply

Anonymous May 6, 2016 at 4:07 AM

This comment has been removed by a blog administrator.

Reply

Unknown May 11, 2016 at 1:02 AM

This comment has been removed by a blog administrator.

Reply

Unknown May 13, 2016 at 1:47 AM

This comment has been removed by a blog administrator.

Reply

Unknown May 18, 2016 at 3:10 PM

This comment has been removed by a blog administrator.

Reply

Unknown May 18, 2016 at 8:25 PM

This comment has been removed by a blog administrator.

Reply

Unknown May 26, 2016 at 8:53 AM

This comment has been removed by a blog administrator.

Reply

Unknown May 26, 2016 at 11:03 PM

This comment has been removed by a blog administrator.

Reply

Unknown May 30, 2016 at 8:52 PM

This comment has been removed by a blog administrator.

Reply

chenlili June 3, 2016 at 6:14 PM

This comment has been removed by a blog administrator.

Reply

Unknown June 9, 2016 at 2:11 AM

This comment has been removed by a blog administrator.

Reply

Sanah Winari June 9, 2016 at 9:39 PM

This comment has been removed by a blog administrator.

Reply

Anonymous June 18, 2016 at 5:03 AM

This comment has been removed by a blog administrator.

Reply

Jobsrelease.in June 19, 2016 at 10:08 PM

This comment has been removed by a blog administrator.

Reply

Unknown June 20, 2016 at 6:38 AM

This comment has been removed by a blog administrator.

Reply

Unknown June 26, 2016 at 9:02 PM

This comment has been removed by a blog administrator.

Reply

Unknown June 28, 2016 at 7:27 PM

This comment has been removed by a blog administrator.

Reply

Unknown June 29, 2016 at 7:14 AM

This comment has been removed by a blog administrator.

Reply

Unknown June 29, 2016 at 2:09 PM

This comment has been removed by a blog administrator.

Reply

Unknown June 30, 2016 at 11:46 PM

This comment has been removed by a blog administrator.

Reply

Unknown July 1, 2016 at 4:45 AM

This comment has been removed by a blog administrator.

Reply

Unknown July 2, 2016 at 2:30 PM

This comment has been removed by a blog administrator.

Reply

Unknown July 6, 2016 at 2:04 AM

This comment has been removed by a blog administrator.

Reply

Anonymous July 6, 2016 at 10:30 AM

This comment has been removed by a blog administrator.

Reply

Dr. Powell Garcia July 6, 2016 at 11:58 AM

This comment has been removed by a blog administrator.

Reply

Enter your comment...

Comment as: xcell.xcellula

Sign out

Publish Preview

Notify me

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)