



Let's build a cellular modem based on an unlocked, fully documented chipset that runs free firmware!

The big problem

Aren't you tired of cellular phones (smart or otherwise) that spy on you? Did you know that with almost all "modern" phones a skilled hacker or an overzealous government can hack into your phone over the air and not only siphon off all of your contact lists and pictures and what have you, but also surreptitiously turn on the microphone - without you ever knowing it - and listen in on whatever is happening at your dinner table, in your living room, in your bedroom or wherever your phone happens to be when, as far as you know, it's just sitting idle? These same spying phones also *actively volunteer* your exact GPS location (much more precise than needed for cellular network operation) to any hacker or governmental entity who knows how to request it - and there is absolutely no way to disable this self-incrimination feature.

The reason why these corporate-made phones are able to betray the interests of the end user and serve someone else's interest instead is because they run proprietary software, also known as firmware. Proprietary software is software that is owned and controlled by someone other than its user, with the user being denied the ability to understand how it works, let alone modify or improve it.

A better way

Over the past decade a few small companies and community initiatives have tried to fix the problem

of phones running proprietary software that works against the user. But only one of them got it right: [Openmoko](#). The original Openmoko GTA01 and GTA02 phones whose production ended in 2009 had a vitally important user freedom and empowerment feature which is completely missing in all of the more recent projects and designs: a baseband processor that can run free software (firmware) instead of the proprietary kind.

Many community long-timers are familiar with the word "baseband", and cringe upon hearing it. The so-called baseband processor, also known as the modem or the radio processor, is the part of every cellular phone (smart or otherwise) that is responsible for connecting to the cellular network and making the device work as a phone. The reason why a lot of us cringe at hearing that word is because traditionally these cellular basebands have been the bastion of closedness and proprietary software. In every phone that has ever been made to the present day with the single exception of Openmoko GTA01/02, the baseband is the most closed and proprietary component, the component whose internal operation the user is absolutely forbidden from understanding, let alone improving. It is also naturally the component that is ideally suited for the insertion of privacy-violating backdoors by various shady entities.

The reason why Openmoko's baseband is so special and so different is because it was built using chips from Texas Instruments, as opposed to Qualcomm or Mediatek. The latter two companies are the ones that make the baseband processor chips used in virtually all mainstream phones made today. The prospects for being able to run free software (the kind of software that protects and empowers you instead of spying or otherwise working against you) on chips made by Qualcomm or Mediatek (and thus on any phone built with those chips) are extremely bleak: absolutely no technical documentation for the workings of these chips is available to mere mortals, and even if we got our own free firmware image built, the chip will most likely refuse to run it by way of its cryptographically locked bootloader.

But the older baseband chips from TI that were used by Openmoko are different in two major ways:

1. These chips were made before cryptographically locked bootloaders were invented, hence they lack this malicious feature;
2. Through what may have been an act of divine intervention - we may never know - we, the free software community, now possess **all** technical documentation that is necessary in order to run our own free software on these GSM baseband chips from TI, 100% complete - and we even have the full source code for TI's official firmware to use as a reference. (All materials in question are [gathered on our FTP site](#).)

While Openmoko, back in the days when they existed as a company and produced phones, shipped their phones with an official baseband firmware version that was just as proprietary as any other, they did so only because of legal restrictions, and any end user can very easily replace this proprietary baseband firmware with a [free version](#).

The problem WE need to solve

What Openmoko produced in the late 2000s seems like the perfect solution to the problem of closed proprietary phones with closed proprietary basebands - but there is one problem with this solution. The problem is that Openmoko phones are no longer made: the last production batch was in 2009,

and all remaining surplus has now been fully exhausted - and none of the newer post-Openmoko initiatives have retained the feature that matters, Openmoko's Calypso modem.

The solution to THIS problem is obvious: we need to produce a series of new phones with the same TI Calypso baseband as used by Openmoko, the only cellular baseband chipset that currently exists in the world that can run fully free, fully functional firmware as opposed to the closed and proprietary kind. (The chips themselves are still available as surplus on the Chinese markets in very large quantities.)

What we are doing

Our long-term goal is to produce an entire family of GSM phone/modem devices that are based on the Calypso chipset and thus can run free firmware. (In fact, free is the only kind of firmware that will ever exist for our devices - no proprietary firmware is possible, as we are buying the chips on the surplus market and NOT entering into any NDAs with anyone.) The devices we envision producing include:

- A basic non-smart phone for those who dislike smartphones, yearn for a simpler phone that is specifically designed for talking to human beings rather than data, but wish to be free from proprietary software and from being spied upon.
- A free-software baseband modem module that can be incorporated into free-software [smartphone designs by other teams](#).
- A standalone GSM/GPRS modem (with additional sweet capabilities like [CSD](#)) for use with laptops, with either USB or plain old serial interface.

But we need to start small. Right now we are working toward building our first proof-of-concept modem prototype, which will simply be the modem section of Openmoko's GTA02 phone extracted and separated from the rest of the design and built on a board by itself. It'll be powered from a lab bench power supply emulating the battery and both Calypso UARTs (interfaces for programming, control and data) will be brought out on headers.

We seek to replace Openmoko's triband radio front-end with a quadband one (making a GSM device anything less than quadband means that someone would have to be excluded, and we do not wish to exclude anyone), and this prototype board we currently seek to build will allow us to validate and prove our quadband design before we reuse it as a building block for more complex hardware designs approaching a final product.

We are a non-profit organization (although unfortunately not officially recognized as such yet), and we do *not* believe in the doctrine of "intellectual property". Absolutely everything we have produced in the past and will produce in the future, including the present family of projects, is in the public domain, free for anyone in the world to use as they see fit without asking us for permission. We apply this principle not only to software, but also to hardware: all design work is being done in public source repositories, and whenever we have a board design ready to be physically produced, we release the finished schematics, BOM, gerber files and editable PCB sources into the public domain via our FTP site. In other words, we create a ready-to-build design, but absolutely do not mind if someone else takes our work and runs with it into commercial production. We *want* you to

"pirate" our work!

Free firmware choices

The Free Software community greatly values diversity and freedom of choice, and free firmware for phones with Calypso baseband processors is no exception. At the present time there is not just one but two independent free software projects seeking to produce fully free and fully functional GSM baseband firmware that can replace the proprietary kind: one is our own [FreeCalypso](#) and the other is [OsmocomBB](#). The two free firmware projects have somewhat different focus: OsmocomBB focuses on facilitating GSM hacking and security research, whereas our own FreeCalypso project seeks to produce free firmware for everyday use by ordinary end users.

When we build our own Calypso phones and modems that will run free firmware on the baseband processor, the choice of *which* free firmware to run remains with the user. While we naturally promote and support our own implementation, there will never be any obstacle to running OsmocomBB (or any other free firmware implementation that may appear in the future) on our hardware.

Our qualifications

The principal developer behind this project has been working toward the goal of a cellular phone free from proprietary software since 2011. Between 2011 and 2013 I gathered (through painstaking and meticulous scavenging) the most critical parts of our extensive collection of hardware documentation and reference source code that is now [amassed on our FTP site](#) (it never stops growing though), and since 2013 I've been working on the free firmware project linked above.

But software/firmware work alone can only take us so far: now that the supply of pre-existing phones with the Calypso baseband chipset has been exhausted, it is time for us to build our own hardware with this chipset in order for the world at large to be able to benefit from our work.

In the case of Open Source Hardware development, my experience is that I have designed and built my own SDSL modem that serves my own Internet connection; you can read about that project, download all related design files (released free to the world as always) and see pictures of the gadget [here](#). Thus I consider myself as qualified as anyone else for the job of building phones and modems with a free Calypso baseband.

What we need money for

As explained above, the first milestone we are pursuing in the hardware subproject of FreeCalypso is to build a small PCB containing a circuit equivalent to the Calypso modem block of Openmoko phones, but made standalone and quadband instead of triband. We already have the schematics and BOM data recaptured in our own free EDA system, and we are almost ready to start PCB layout. However, there are two steps which we need to complete first before we can start our own layout, and which require money:

1. We really need to use Openmoko's modem section layout as a reference for our own, i.e., we need to base our own PCB layout on a known-working reference. However, the original

GTA02 PCB layout files from the golden days of Openmoko appear to have been irretrievably lost. Therefore, we need to recover the lost PCB layout by reverse engineering. There is [a company in Colorado](#) who can do just what we need - professionally recover the entirety of the lost PCB layout from a sacrificial board - but it will cost about \$6000.

2. We already have most of the parts needed for the Calypso modem block, including all of the core TI chips, but there are a few more parts we need to buy from our Chinese aftermarket supplier. The anticipated cost is around \$900.

Thus the total budgetary need to get our project rolling toward our first hardware milestone is \$6900; the campaign goal has been set to \$7500 to account for the Indiegogo platform and payment processor fees.

What we promise to deliver

If we reach our funding goal, we shall promptly do the following in this order:

1. Send our sacrificial GTA02 board to Colorado for professional PCB reverse engineering;
2. Publish the results of this reverse engineering (high-resolution scans of each copper layer, both outer and inner, aligned and calibrated) free to the world on our FTP site;
3. Using the reverse-engineered GTA02 layout as a reference, create our own layout for the standalone quadband GSM modem board we seek to build. Our own layout will be done in GNU PCB (bona fide free software EDA tool with a simple and fully documented text-based file format), and all design files will be released free to the world, so that the physical production can be done not only by us, but by anyone in the world.

If we fail to reach our funding goal, we shall hold on to whatever money we manage to raise and wait indefinitely until we are able to supplement it with our own personal funds to reach the goal of being able to pay for the reverse engineering of the GTA02 PCB.

If we exceed our funding goal, any money raised beyond the cost of GTA02 PCB reverse engineering and the cost of the parts we need to buy will be applied to other future project costs which are not yet known.

\$220USD

raised of \$7,500 goal

3%

29 days left

This campaign started on Apr 05 and will close on May 05, 2015 (11:59pm PT).

Flexible Funding

Select a contribution amount below:

\$1

\$50

\$100

USD

[Contribute Now](#)

Select a Perk

Help make it happen
for Free Software Cellular Baseband and the team!