Un-boxing the infamous CTF location tracker

rtr, 14th March 2015

On March 4th, 2015, a tracking device was found inside of the wheel well of a car belonging to an attendee of the Circumvention Tech Festival in Valencia, Spain. A few pictures of the device have been made available online. The picture shows how the components of the tracker are concealed with black epoxy that is used to goop the circuitry.

Image: Tracker dissembled and placed in the vehicle

During the past week, we have reviewed the pictures and reached the following conclusions:

- **What components are used in the tracking device?**
  The tracking device is composed of four functional blocks: (a) a voltage regulator, (b) a GSM/GPRS modem from Wavecom/Sierra Wireless, (c) a GPS receiver from Ublox and (d) a micro controller unit (MCU) possibly from Renesas. The circuit has two separate antennas to interface with the mobile operator (Movistar) and the GPS satellites. An external battery back provides power to the unit.

- **Is the device state-of-the-art in location tracking?**
  No, Judging by the type of components included in the tracker, the unit is rather old (5-7 years) as the level of circuit integration of GPS/GSM available in the market in the last years is much higher. For example, Combo antennas that both work in GSM and GPS are available and for example Telit sells a ultracompact GSM/GPRS single module (GE864-GPS).

- **Is such big battery back needed?**
  While the Micro Controller Unit included in the device has low power consumption and "Stand by" functionalities there are plenty of better low power alternatives. The processor included in the design is not common in low cost GPS tracking devices that include ARM 32-bit Cortex -M3 CPU. This makes me believe that the device was not originally designed to be attached to a small battery pack but rather connected to a car battery or other source of constant power.

- **What about the two lithium batteries?**
  The two lithium batteries present in the board provide power to the Real Time Clocks (RTCs)

of the GSM module (Ublox Neo-6M) and the Micro Controller. The big 3V CR2032 battery that covers the Micro Controller seems oversized and could indicate the presence of a logic to detect the disconnection of the battery pack that could eventually wipe out any data in the device.

- **How is the tracker configured?**
  The board lacks an obvious interface port (JTAG, USB, etc) to program the unit and the programming could just take place via SMS or commands send to the unit via GPRS.

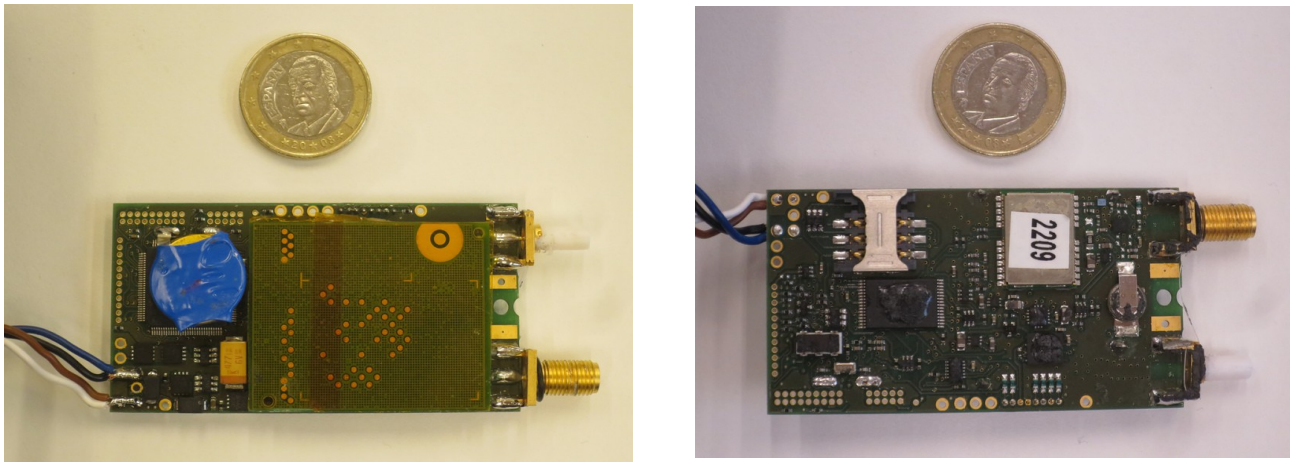

Image: Front and Back side of the infamous tracker

Functional Blocks

The board is composed of four large functional parts

(a) Power

The unit is fed with four D size batteries (aka as IEC R20 batteries). The four batteries are in a serial configuration to supply 6 volts to the board. The yellow component marked as (447 6V) is a TAJD447K006, a tantalum capacitor.

Two batteries are present in the board. The two lithium batteries (CR2016/2032) provide 3-3.6V volts to the real time clocks (RTC) of the GPS and the Micro Controller Unit (MCU). The small round battery allows to store in the internal memory of the GPS module the last position recorded in case of power loss. The presence of an external battery connected to the Micro Controller Unit (MCU) provides the possibility to detect the disconnection of the battery pack.

(b) GSM/GPRS modem

The connection to the mobile phone network is implemented with a Wavecom/Sierra Wireless AirPrime GSM/GPRS Wireless Control Module (model number Q2687RD). The modem provides access to the mobile network, this modem is quad-band and can operate in 850, 900, 1800 and 1900 MHZ. The SIM card is from Movistar, the major Spanish mobile phone operator owned by Telefónica S.A. The modem uses the 2G network (GPRS).

The board includes this modem without the stickers that normally include the Equipment Identifier or IMEI.

Image: Wavecom GPRS Modem

(c) GPS modem

The third functional block is the GPS modem, the modem obtains location information via GPS and pushes such information to an external location using the mobile network. The modem is a ublox GPS modem, probably the NEO 6 Series.

Image: Traditional built-in ceramic antenna and ublox GPS receiver

The board includes the ublox GPS receiver without the sticker.

The receiver does not include a built-in antenna, portable GPSs normally include a ceramic antenna like the one in the picture or high gain external antenna. Instead the GPS is connected to phantom external antenna with magnet base.

(d) Micro-controller Unit (MCU)

The forth functional block is the micro controller unit (MCU), the CPU of the location tracker. The MCU's responsibility is to interface with both the GPS receiver and the GPRS modem. It is difficult to determine the brand of the MCU without physical access to the board but we know that the MCU has 120 pins, that is a Thin Quad Flat Pack (TQFP). This package (form factor) assembles the MCUs manufactured by Renesas.
In this functional block can we also find a 32-pin NAND memory flash.

Rtr, 14th March 2015 rtr@nodo50.org