“THE BICHO”

AN ADVANCED CAR BACKDOOR MAKER

ABSTRACT

Attacks targeting connected cars have already been presented in several conferences, as well as different tools to spy on CAN buses. However, there have been only a few attempts to create “something similar” to a useful backdoor for the CAN bus. Moreover, some of those proofs of concept were built upon Bluetooth technology, limiting the attack range and therefore tampering its effects.

Now we are happy to say that: Those things are old!

Throughout our research we have successfully developed a hardware backdoor for the CAN bus, called *"The Bicho"*. Due to its powerful capabilities we can consider it as a very smart backdoor. Have you ever imagined the possibility of your car being automatically attacked based on its GPS coordinates, its current speed or any other set of parameters? *The Bicho* makes it all possible.

All this "magic" is provided by the assembler-coded firmware we developed for a PIC18F2580 microcontroller. Additionally, our hardware backdoor has an intuitive graphical interface, called "Car Backdoor Maker", which is open-sourced and allows payload customization. *The Bicho* supports multiple attack payloads and it can be used against any vehicle that supports CAN, without limitations regarding manufacturer or model. Each one of the payloads is related to a command that can be delivered via SMS, this way it allows remote execution from any geographical location.

Even more, as an advanced feature, the attack payload can be configured to be automatically executed once the target vehicle is proximate to a given GPS location. The execution can also be triggered by detecting the transmission of a particular CAN frame, which can be associated with any given factor, such as: the speed of the vehicle, its fuel level, and some other factors. This feature provides the means to design highly sophisticated attacks and also being able to execute them not only remotely but also automatically.

TECHNICAL DETAILS

Our project is divided in two parts: the *"Car Backdoor Maker"* (PC software) and *"The Bicho"* (hardware-backdoor for CAN bus). Both are Open Hardware/Source.

The *Car Backdoor Maker* has an intuitive graphical interface that allows payload customization for using with the hardware-backdoor.

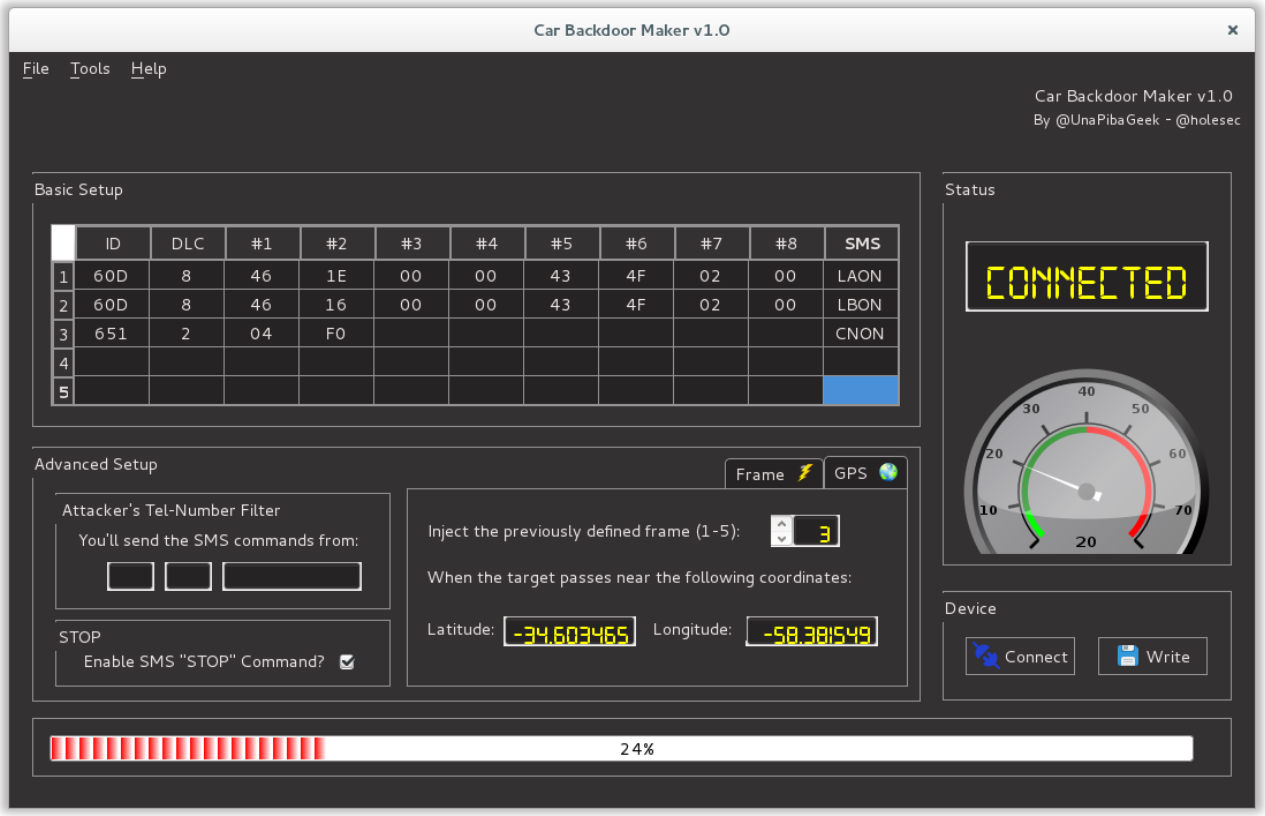


Figure 1. Car Backdoor Maker GUI.

Its main features are the following:

- Connects to the *hardware backdoor* via USB.
- Set up different (up to five) CAN frames (payloads) to be injected remotely.
- Set up the SMS command for executing each payload.
- Set up a Tel number that will be used to send the SMS commands.
- Set up the GPS coordinates where a payload must be executed.
- Set up a specific CAN frame as a parameter for the automatic injection of a payload.
- Download all the attack parameters to the hardware backdoor with just a click.

On the other hand, “The Bicho” is the hardware backdoor. It has a PIC18F2580 microcontroller and all the "magic" is in the assembler-coded firmware we developed for it. The microcontroller is responsible for injecting the frames in the CAN bus according to the information it receives from a SIM800L (SMS Commands / GPS coordinates).

Additionally, the hardware has an USB interface to connect to the PC in order to be configured through the "Car Backdoor Maker" software. Another important component is the connector, which has four pins: two of them for the power (provided by the vehicle's OBD-II port); and two more for the CAN HIGH and CAN LOW signals which go through pins 6 and 14 of the OBD-II port.

Once it has been connected to the CAN bus, the hardware backdoor is also able to access the CAN bus frames, that´s the reason why it can also be configured to perform an injection (attack) automatically when a specific state-related frame is detected.

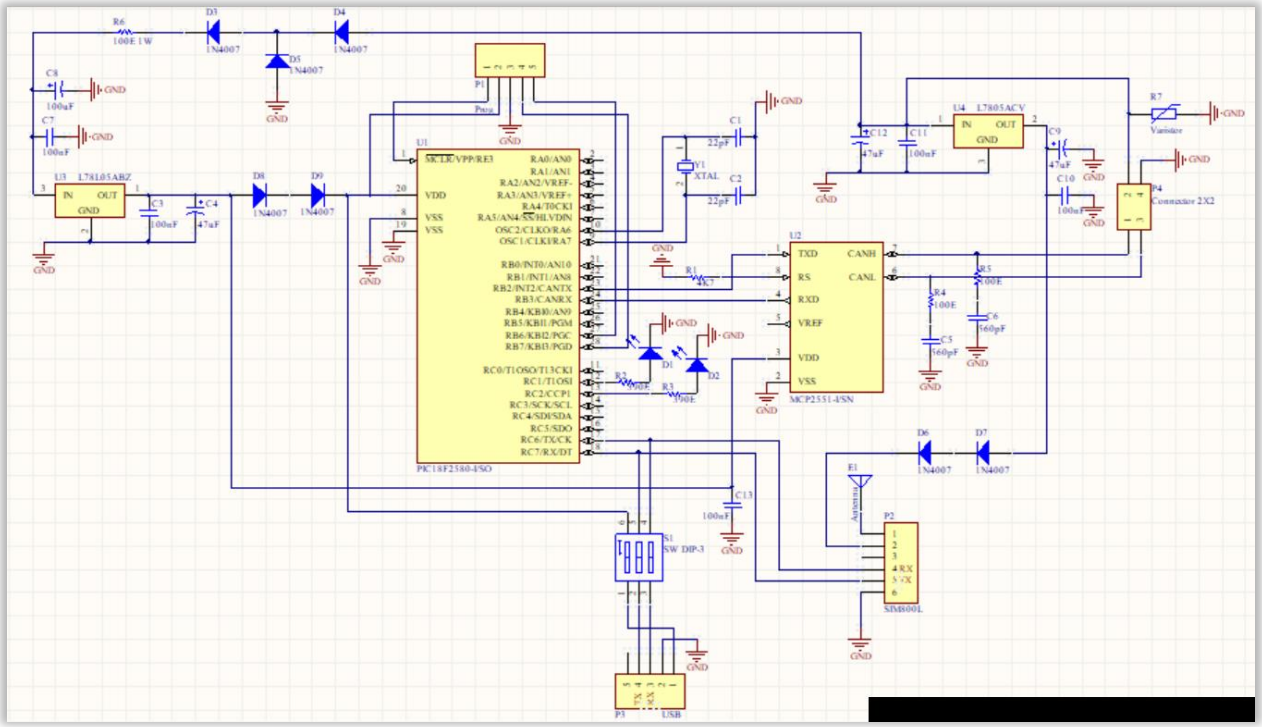


Figure 2. The Bicho hardware schematics.

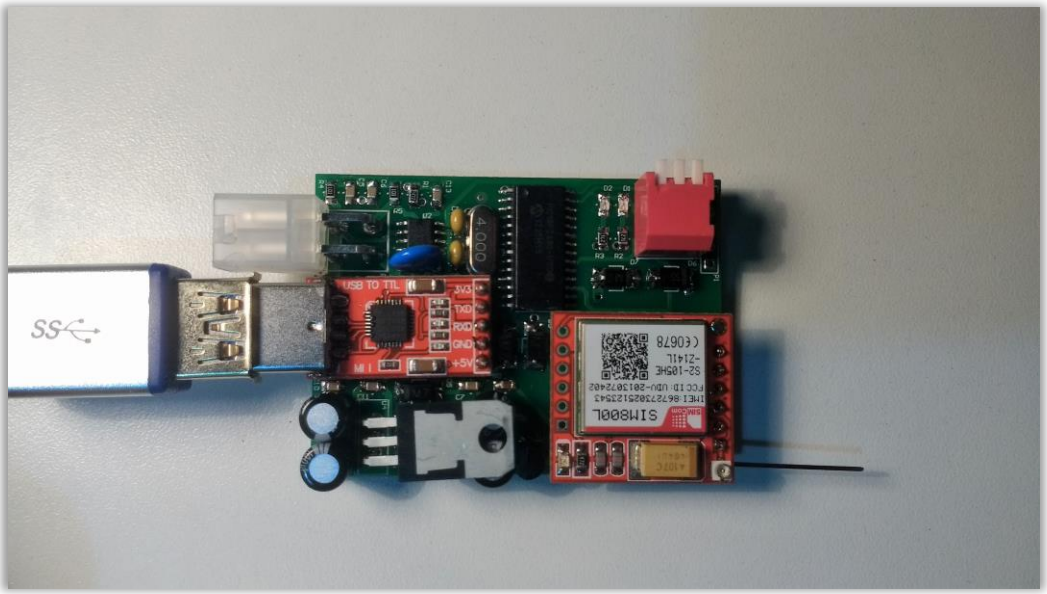


Figure 3. The Bicho connected to the USB to be programmed.

INSTALLATION

After using the *Car Backdoor Maker* for loading the attack payloads on *The Bicho*, the only thing the user needs to do is to connect *The Bicho* to the OBD-II port of the target car (hopefully, their own car). Such port is usually exposed and easy to find below the steering wheel, so finding it and connecting the hardware backdoor requires only a few seconds.

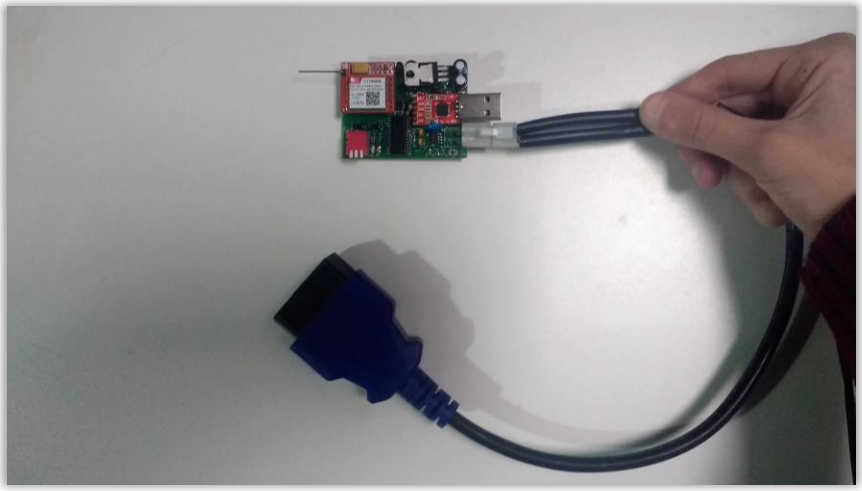
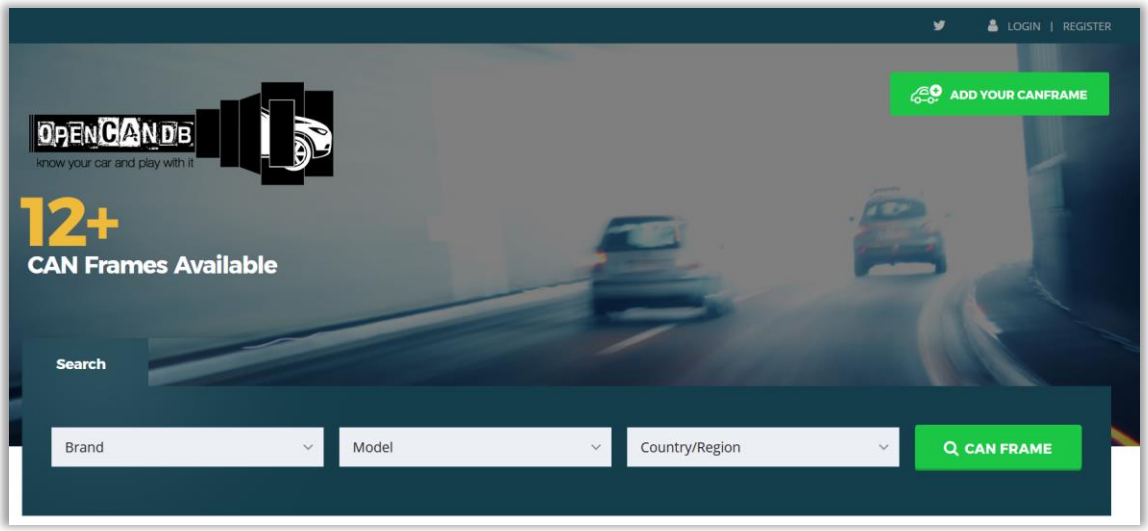


Figure 4. The Bicho with the OBDII connector.

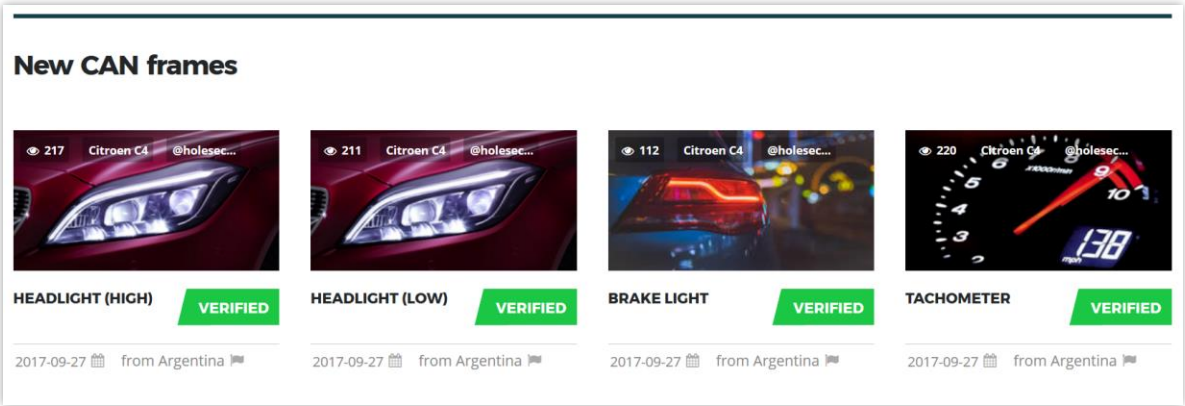
OPENCANDB

Keep in mind every manufacturer uses their own CAN frames for each car model, the great question is: How can I find the CAN frame I need? One way is through a reversing process, but such process could be so hard and it is necessary to have all the car you want to research.

To solve this, we are releasing a new project called “OpenCANdb”, where users can find out any frame they want, download and use it in the *Car Backdoor Maker* or any other tool, just with a simple search.



As it’s show in the image above, we have filters by manufacturer, car model and country. Everyone can upload CAN frames and share them with all.



We are sure that it will be a useful tool for every car hacker. The *OpenCANdb* is available at the following website: www.opencandb.online.

CONCLUSIONS

As an example, consider the following case:

Let´s assume you know the CAN frame for the throttle position of the target car (or you got such CAN frame from OpenCanDB).

One way of attack would be using that frame with *The Bicho* to remotely alter the car's speed through SMS commands.

Another way would be using the advanced features of the backdoor to alter the speed automatically (with *The Bicho*) once the car reaches a specific state (GPS coordinates or any other parameter).

Achieving this is easy for anyone using the *Car Backdoor Maker*, this software will upload the payload to The Bicho via USB, and it'll be ready to connect to the OBD-II port of the target car and *take action*.

Our tool is not hacker-priced, nor corporation-priced; you can find the sources and more information at: https://github.com/UnaPibaGeek/CBM.

Claudio Caracciolo – Sheila A. Berta.