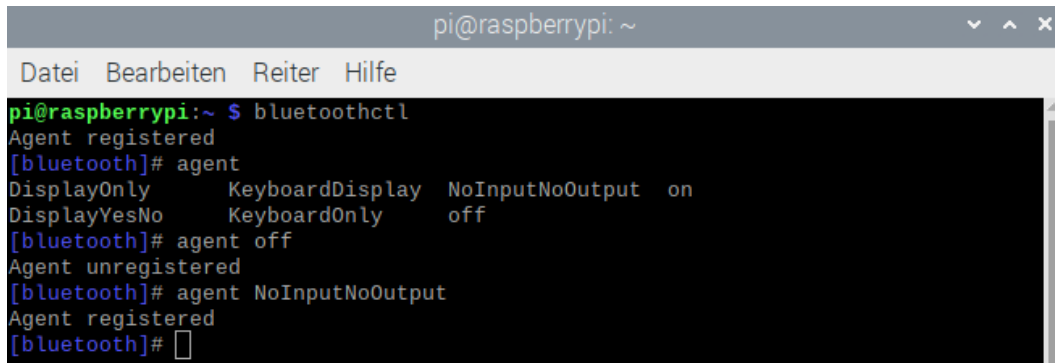


BT-Niño-MitM Attack

I only needed to make some changes in the Bluetooth configuration of the Raspberry Pi for this attack. The kernel remained unchanged. For this attack, I used the kernel version *v 5.15.32*.

To set the I/O capability to `NoInputNoOutput` instead of the preconfigured one, `KeyboardDisplay`, I used the `bluetoothctl` utility from the `bluez-utils` package. I started this utility by typing `bluetoothctl` in the command line which automatically starts an agent which is responsible for managing the Bluetooth *pairing code*. I first deregistered the agent by typing `agent off`. Then I registered it again, but with the I/O capability `NoInputNoOutput` by typing `agent NoInputNoOutput`. A summary of this process can be seen in figure 1 [?, ?].



```
pi@raspberrypi: ~  
Datei Bearbeiten Reiter Hilfe  
pi@raspberrypi:~ $ bluetoothctl  
Agent registered  
[bluetooth]# agent  
DisplayOnly          KeyboardDisplay  NoInputNoOutput  on  
DisplayYesNo         KeyboardOnly    off  
[bluetooth]# agent off  
Agent unregistered  
[bluetooth]# agent NoInputNoOutput  
Agent registered  
[bluetooth]#
```

Figure 1: bluetoothctl settings