Elm-327 clone device

Ludvig Christensen and Daniel Dannberg
KTH Royal Institute of Technology, Stockholm Sweden
2019

Security research was made on a device called elm327, which turned out to be a clone[1][2], and we came to the conclusion that it is a very insecure unit. The unit comes with a hardcoded password which was on the extreme low in terms of security. But what is alarming with the device is that there seems to be a possibility to send arbitrary commands/messages to the car's ECU using it. A service such as pythonOBD[3] makes the process easy. Researchers have showed that if you know the specific car CAN message then you can use functions that are not supposed to be enabled such as turning of lights[4]. One limitation of the device is that its performance isn't enough to sniff messages from the CAN bus. This means that to send commands one would need to know them for the specific car the device is plugged into beforehand. A security precaution for this specific device is to simply unplug it from the OBD-II port, since it's not possible to change the hardcoded password. We did not explore the device's function in regards to being turned on when the car is turned off. Assuming the worst it's best to remove it from the port when not in use.

[1] https://www.teknikmagasinet.se/produkter/halsa-fritid/outdoor/biltillbehor/elm327-obd2-bluetooth
[2] https://en.wikipedia.org/wiki/ELM327#Pirate_clones
[3] https://python-obd.readthedocs.io/en/latest/Command\%20Tables/
[4] http://www.autosec.org/pubs/cars-oakland2010.pdf