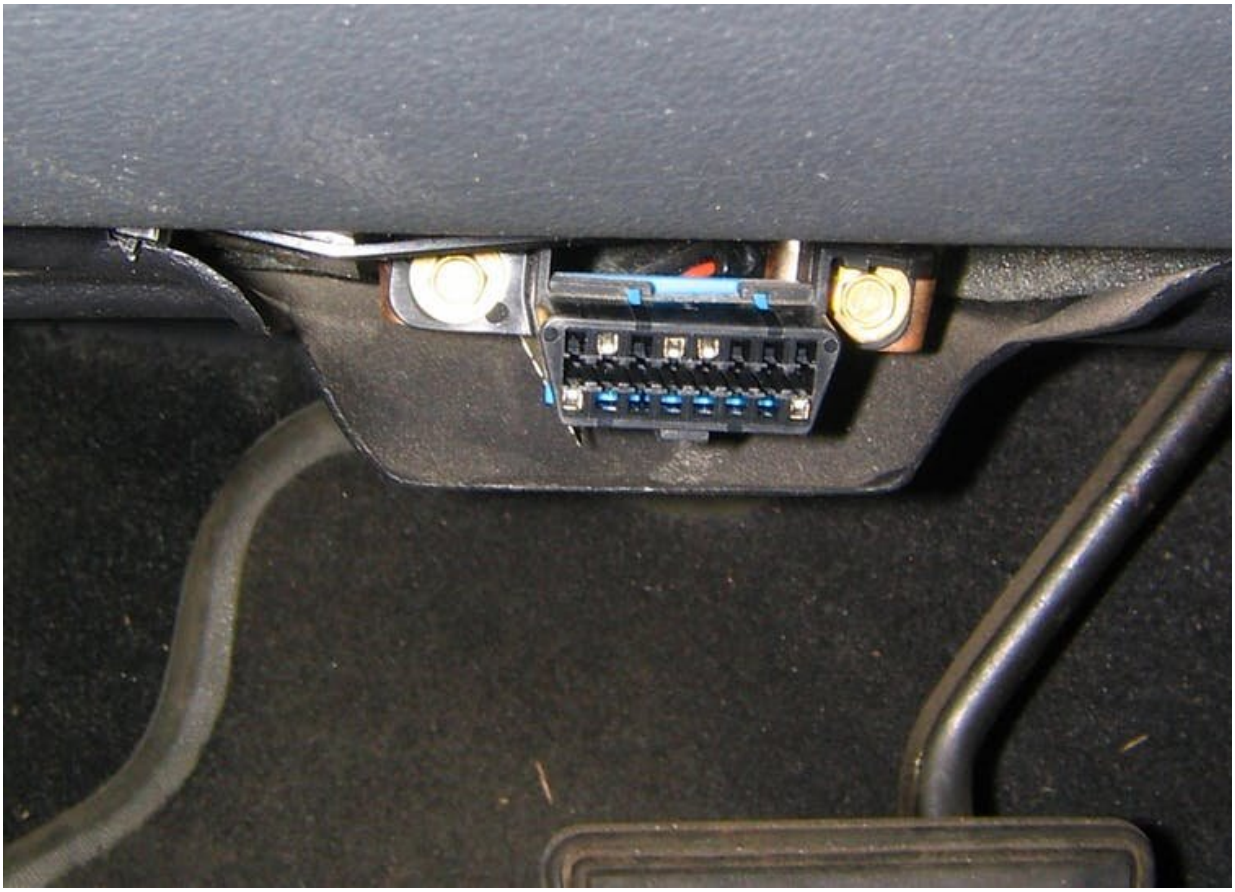
Your car is more likely to be hacked by your mechanic than a terrorist

March 1 2019, by Richard Matthews



An example of an On Board Diagnostic (OBD) port in a car. This port is normally under the steering wheel. Credit: endolith/flickr

When it comes to car hacking, you should be more worried about dodgy

dealers than one-off hackers with criminal intent.

Hollywood would have us believe our cars are extremely vulnerable to hackers. A hacker remotely logs into the onboard computer of a car on display in a showroom, causing the car to burst through the glass out onto the street – just in the nick of time to block a car chase.

And researchers have had some success replicating such a scenario. In 2015, headlines were made all over the world when security researchers were able to hack a Jeep Cherokee. They remotely controlled everything from windscreen wipers and air conditioning to the car's ability to accelerate. Ultimately they crashed the car on a nearby embankment, safely ending their experiment.

If you believed everything that has been written since, you would think we are all driving around in accidents waiting to happen. At a moment's notice any criminal could hack your vehicle, seize control and kill everyone inside.

While this threat may exist, it has never happened in the real world – and it's significantly overhyped.

Cars are now controlled by computers

Today's motor vehicles are a complicated system of interconnected electrical sub-systems, where traditional mechanical connections have been replaced with electrical counterparts.

Take the accelerator, for example. This simple device used to be controlled by a physical cable connected to a valve on the engine. Today it is controlled by drive-by-wire system.

Under a drive-by-wire system, the position of the throttle valve is

controlled by a computer. This computer receives signals from the accelerator and correspondingly instructs a small motor connected to the throttle valve. Many of the engineering benefits are unnoticed by a typical consumer, but this system allows an engine to run more smoothly.

A failure of the drive-by-wire system was suspected to be the cause of unintended acceleration in 2002 Toyota vehicles. The fault resulted in at least one fatal crash, in 2017, being settled outside of court. An analysis commissioned by the US National Highway Traffic Safety Administration could not rule out software error, but did find significant mechanical defects in pedals.

These were ultimately errors in quality, not hacked cars. But it does introduce an interesting scenario. What if someone could program your accelerator without your knowledge?

Hack the computer and you can control the car

The backbone of today's modern interconnected vehicle is a protocol called a Controller Area Network (CAN bus). The network is built on the principle of a master control unit, with multiple slave devices.

Slave devices in our car could be anything from the switch on the inside of your door, to the roof light, and even the steering wheel. These devices allow inputs from the master unit. For example, the master unit could receive a signal from a door switch and based on this send a signal to the roof light to turn it on.

The problem is, if you have physical access to the network you can send and receive signals to any devices connected to it.

While you do need physical access to breach the network, this is easily accessible via an onboard diagnostic port hidden out of sight under your

steering wheel. Devices such as Bluetooth, cellular and Wi-Fi, which are being added to cars, can also provide access, but not as easily as simply plugging in.

Bluetooth, for example, only has a limited range, and to access a car via Wi-Fi or cellular you still require the vehicle's IP address and access to the Wi-Fi password. The Jeep hack mentioned above was enabled by weak default passwords chosen by the manufacturer.

Enter the malevolent mechanic

Remote car hacks aren't particularly easy, but that doesn't mean it's OK to be lured into a false sense of security.

The Evil Maid attack is a term coined by security analyst Joanna Rutkowska. It's a simple attack due to the prevalence of devices left insecure in hotel rooms around the world.

The basic premise of the attack is as follows:

- the target is away on holiday or business with one or more devices
- these devices are left unattended in the target's hotel room
- the target assumes the devices are secure since they are the only one with the key to the room, but then the maid comes in
- while the target is away, the maid does something to the device, such as installing malware or even physically opening up the device
- the target has no idea and is breached.

If we look at this attack in the context of the CAN bus protocol it quickly becomes apparent the protocol is at its weakest when physical access is granted. Such access is granted to trusted parties whenever we

get our vehicles serviced, when it's out of our sight. The mechanic is the most likely "maid".

As part of a good maintenance routine your mechanic will plug a device into the On Board Diagnostic (ODB) port to ensure there are no fault or diagnostic codes for the vehicle that need to be resolved.

But, what would happen if a mechanic needed some extra business? Perhaps they wanted you to come back for service more often. Could they program your electronic brake sensor to trigger early by manipulating a control algorithm? Yes, and this would result in a lower life for your brake pads.

Maybe they could modify one of the many computers within your vehicle so that it logs more kilometres than are actually being done? Or if they wanted to hide the fact they had taken your Ferrari for a spin, they could program the computer to wind back the odometer. Far easier than the manual method, which ended so badly in the 1986 film Ferris Bueller's Day Off.

All of these are viable hacks – and your mechanic could be doing it right now.

The case for verification and transparency

This isn't a new problem. It's no different from a used car dealer using a drill to run the speedo back to show a lower mileage. New technologies just mean the same tricks could be implemented in different ways.

Unfortunately, there is little that could be done to prevent a bad mechanic from doing such things.

Security researchers are currently focused on improving the security

behind the CAN bus protocol. The likely reason no major incident has been reported to date is the CAN bus relies on its obscure implementation for security.

Verification and transparency could be a solution. A system, proposed by researchers at Blackhat, involves an audit log that could assist everyday people in assessing the risks to any unauthorised changes to their vehicle, and improve the robustness of the system.

Until then, we will just have to keep using a trusted mechanic.

Provided by The Conversation