Computerised vehicles are vulnerable to hacking and theft

January 27 2015, by Andrew Smith And Blaine Price

Who's really driving your car? Credit: Saad Faruque, CC BY-SA

Theft of vehicles is about as old as the notion of transport – from horse thieves to carjackers. No longer merely putting a brick through a window, vehicle thieves have continually adapted to new technology, as demonstrated by a new method to steal a car without the need to be anywhere near it.

Modern vehicles are built with a range of computerised systems that control and monitor security, fuel, engine management and more. Most new cars are fitted with Bluetooth connectivity and USB sockets, so it was only a matter of time before reports of criminals abusing these systems appeared. The use of so-called Bad USB memory sticks to hijack systems has been reported, but the most recent issue involves a port fitted in virtually every car on the road today, the 30-year-old On-Board Diagnostic port (OBD-II). So put away that coat hanger – car theft has got a lot more technological.

Fleet attacks

At the recent S4 security conference, researcher Corey Thuen shared his concerns regarding a specific OBD-II dongle provided by US insurer Progressive Insurance. Designed to track driving habits, the dongle "phones home" to report back to the company via the mobile phone network, and the driver is awarded a lower premium if his or her driving habits demonstrate no dangerous driving – speeding, hard accelerating or breaking.

Unfortunately the port also provides read and write access to the car's engine management system. If a remote attacker was able to use a man-in-the-middle attack – intercepting traffic between the car and the company's servers while passing themselves off as one or the other – they could compromise the dongle, and so have complete control over the car's engine. Potentially this attack could compromise not just a single vehicle but potentially fleets of vehicles, depending on what data was exposed from the company's servers.

The main issue is for manufacturers to design products with security in mind, and provide updates swiftly once security flaws and vulnerabilities such as these are discovered. Some manufacturers are much better at doing so than others.

In this case, the dongle does not attempt to validate or demand signed firmware updates, its boot process is not secure, it doesn't authenticate the mobile phone connection, nor encrypt the data it sends, nor is it hardened in any way against potential attacks. "Basically it uses no security technologies whatsoever," Thuen remarked. It's essentially an open door.

Malware in disguise

Other security compromises based on computer systems in cars include using Bluetooth MP3 players, where malware disguised as a music track is loaded into the car's systems to compromise them, or through applications on smart phones that use the Bluetooth connection to access the car's systems.

On top of the distinctly disturbing idea of your car being hijacked and remotely controlled, there are also privacy concerns about the data the car collects about you. As well as information about driving habits, GPS data can locate you and build a pattern of your comings and goings, posing further risks.

There's long been a problem here due to closed, proprietary systems to which you the owner and user don't have access – something Open Rights campaigners such as the journalist Cory Doctorow have noted.

What can you do?

Usually security advice includes not clicking on dodgy links, and keeping your antivirus and other software up-to-date. But with a car you are choosing to place your body inside a one-tonne computerised cage travelling at 100 km/h, which may no longer be in your control.

The solution, long understood by security researchers, is that software needs to be open to inspection so that bugs and flaws are easier to find and report, and so the software is fixed and improved more quickly. Closed, proprietary software puts users at unnecessary risk by obscuring potential problems that may not be made public, but could equally have been discovered by criminals who are only to happy to exploit them. Drivers need to understand how the modern car has changed and continues to change, and to lobby the car industry to change their approach.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation