The cyber-mechanics who protect your car from hackers

by Chris Baraniuk

New Scientist No. 3033, 8 August 2015

A hacking incident led to the recall of 1.4 million Dodge, Jeep, Ram and Chrysler vehicles.

A couple of weeks ago, a small team of security researchers gathered near a car parked outside one of their company’s buildings. The vehicle was on loan to them from a carmaker, and the goal was to find out how hackable it was.

The team did not need to physically connect to the vehicle or even enter it – they simply jacked in over Wi-Fi. When they did, they soon found an unexpected vulnerability.

“There was a route through to the vehicle network where the more sensitive, safety critical systems are,” explains Andy Davis of NCC Group, an information security specialist based in Manchester, UK. He says his team could have used this security breach to fiddle with the car’s automatic braking.

“If someone thought their automated braking was turned on, we could have turned it off without them knowing.”

It’s the kind of penetration test that NCC Group and their partner SBD, an automotive security specialist based in Milton Keynes, UK, do for car companies all the time. In fact, the firms say they carry out work for around 95% of the world’s vehicle manufacturers.

News that security researchers Chris Valasek and Charlie Miller were able to remotely kill the engine of a Jeep while it was on the road made international headlines recently. It also resulted in the recall of 1.4 million vehicles by Fiat Chrysler, which owns Jeep.

Highly secretive

But many people do not realise that car companies are actually doing day-to-day experiments in an attempt to tackle the security issues associated with increasingly high-tech, connected cars. Those in the industry are quick to point out that corporations remain highly secretive about this work for fear of inspiring criminals or giving away technical details to competitors.

“Most manufacturers know there is a problem and they’re working on solutions, but no-one will go public with it,” explains Martin Hunt, who works in automotive penetration testing for UK telecommunications firm BT.

Hunt points out that hackers are often able to gain control of crucial functions in a car – such as braking, steering or switching the engine on and off – through surprising means. A common example is via the in-car “infotainment” system, which provides audio and visual entertainment to passengers.

“Quite often these systems are interconnected via a central control unit. If you can get into one you can get into another,” says Hunt as he points out that practically every function in a car is nowadays connected to a computer that controls not just one aspect of the vehicle, but many.

Essentially, this has led to a broadening of what is known as the car’s “attack surface” – the number of ways it could be hacked.

Although there are no reported cases of criminals using such techniques to maliciously send cars off the road just yet, Davis thinks that exploits that could be quickly monetised – such as unlocking and stealing parked cars – may soon appear.

And his colleague Mike Parris at SBD agrees. “With connected cars becoming increasingly popular, my concern is that this picture could change very quickly,” he says.

Black boxes

One individual who has spent the last couple of years trying to get carmakers to wake up to the threat is US-based security researcher Josh Corman, who has set up an initiative, I Am The Cavalry, to improve the public safety of various technologies. He and others have developed a five-point framework to help vehicle manufacturers better adjust to the threats of hacking.

Corman says that progress is being made, and he is now in regular discussions with carmakers about how to implement these ideas. One suggestion is “black boxes” that can record the details of hacking if it does occur on a vehicle, allowing for diagnostics and patches to be developed more quickly afterwards.

But the rapid pace of change in the car sector means that security solutions can lag way behind the vulnerabilities introduced by the latest innovations. Recently, a representative from one firm told Corman that it would take four to five years to introduce black boxes.

“They’re adding attack surfaces at a rate of one a year but telling me it’ll take five years to secure them,” says Corman. “We have a lot of catching up to do.”