Hackers could take control of cars and kill millions, ministers warned

Andrew Ellson, Consumer Affairs Correspondent

November 20 2017, 12:01am, The Times

Modern cars are an “open door” to hackers, inviting hostile states to use Britain’s roads as a weapon against citizens, ministers have been warned.

Deaths are inevitable within five years if carmakers do not fix vulnerabilities in technology, one of the world’s experts in vehicle software has said.

Justin Cappos, a computer scientist at New York University, said that any car built since 2005 could be controlled remotely by hackers with some cars built as long ago as the year 2000 also at risk. Hackers could already be causing accidents without the authorities realising it because no one was looking for the evidence.

The professor said that many lives were at risk and the vulnerability of cars should be an “urgent” national security issue. “If there was a war or escalation with a country with strong cybercapability, I would be very afraid of hacking of vehicles,” he said. “Many of our enemies are nuclear powers but any nation with the ability to launch a cyberstrike could kill millions of civilians by hacking cars. It’s daunting.

“Once in, hackers can send messages to the brakes and shut off the power steering and lock people in the car and do other things that you wouldn’t want to happen.” He wants the government to make software updates mandatory.

Stephen Morrow, of SQS Group, which advises businesses on software protection, said that regulation was essential. “Manufacturers must be accountable. A lot only want to do the minimum — security can be expensive and too many see it only as a tickbox exercise,” he said. “This is serious — lives are at stake. Government is going to have to get involved and standards developed and enforced.”

Carsten Maple, professor of cyber-engineering at the University of Warwick, said: “We’ve already seen vehicles used with devastating effect as weapons. Cybersecurity researchers and industry must ensure that systems are engineered to stop new attacks. This requires us to think as an attacker would, rather than an engineer.”

There are about nine million wifi-connected cars on British roads. Most of these have between 50 and 100 electronic control units — small computers that control one or more systems, such as power steering or brakes. These devices send messages to one another but there is little security between them.

“Once you are in the network you are able to communicate with any device so you could send a message to engage the brakes,” Professor Cappos said. “Components in cars are not good at understanding where messages come from and whether they are authentic.”

The ease with which cars can be hacked was illustrated last year when two researchers remotely took control of a Jeep’s brakes, steering and transmission while it was on the road.

Concerns over hacking are shared by the public. A Populus survey conducted by Comparethemarket.com found that almost 60 per cent of people have little or no confidence that modern cars are safe from cyberattacks. Two thirds think car makers must do more to protect vehicles from hackers.

Despite the perception that the real danger from hacking will be for driverless cars, Professor Cappos said that they would be safer than traditional vehicles because protections such as automatic braking would be built in.

A spokeswoman for the Society of Motor Manufacturers and Traders said: “Billions are invested to stay ahead of criminals and new cars have never been more secure. They are already being equipped with the means to prevent remote hacking through regular software upgrades as well as encryption, layering, and alarms and immobilisers.”

The government said that it had set out principles of cybersecurity that addressed governance and product design.

https://www.thetimes.co.uk/edition/news/hackers-could-take-control-of-cars-and-kill-millions-ministers-warned-fx8gv5sk7