BBC

Car hackers use laptop to control standard car

By Zoe Kleinman
Technology reporter, BBC News

26 July 2013 | Technology

The researchers managed to stop, start and steer a car with an old Nintendo handset

Next time you have a passenger in the back seat of your car offering infuriatingly "helpful" advice about your driving skills, count yourself lucky that they aren't doing anything more sinister in their attempts to guide your vehicle.

Two security experts in the US have demonstrated taking control of

two popular models of car, while someone else was driving them, using a laptop.

Speaking to the BBC ahead of revealing their research at security conference Defcon in Las Vegas in August, Charlie Miller and Chris Valasek said they hoped to raise awareness about the security issues around increasingly computer-dominated car control.

"At the moment there are people who are in the know, there are nay-sayers who don't believe it's important, and there are others saying it's common knowledge but right now there's not much data out there," said Mr Miller, a security engineer at Twitter.

"We would love for everyone to start having a discussion about this, and for manufacturers to listen and improve the security of cars."

Their work, funded by the Pentagon's research facility Darpa, has so far received a mixed reaction from the manufacturers themselves.

How they did it

The researchers used cables to connect the devices to the vehicles' electronic control units (ECUs) via the on-board diagnostics port (also used by mechanics to identify faults) inside a 2010 model Ford Escape and Toyota Prius.

Contained within most modern vehicles, ECUs are part of the computer network that controls most aspects of car functionality including acceleration, braking, steering, monitor displays and the horn.

The pair were able to write software which sent instructions to the car network computer and over-rode the commands from the actual drivers of the cars.

They filmed themselves in the back of one of the vehicles steering it left and right, activating the brakes and showing the fuel gauge drop to zero, all while the vehicle was under driver control and in motion.

A spokesman for Toyota told the BBC that because the hardware had to be physically connected inside the car, he did not consider it to be "hacking".

"Altered control can only be made when the device is connected. After it is disconnected the car functions normally," he said.

The cable used to connect the devices to the ECUs via the diagnostics port.

"We don't consider that to be 'hacking' in the sense of creating unexpected behaviour, because the device must be connected - ie the control system of the car physically altered.

"The presence of a laptop or other device connected to the OBD [on board diagnostics] II port would be apparent."

Expensive and difficult

Mr Miller and Mr Valasek say this is not the point.

Their work builds on earlier research carried out by researchers at the University of Washington and the University of San Diego in 2010, who demonstrated that it was possible to control a car remotely and developed a tool, which they called CarShark, for the purpose.

"We're big fans of their work but we figured they already proved you can remotely get into a car's network," Chris Valasek, director of security intelligence at consultancy IOActive told the BBC.

"We wanted to see how much control would you have once that's happened."

They admitted that they had destroyed a few cars while refining their technique.

I wouldn't dare do this to my own car
Chris Valesek, Car hack researcher

"It's very expensive and difficult to do the research to show you can hack into a car. It's not like you can just download something and look at it," said Mr Miller.

"I wouldn't dare do this to my own car," added Mr Valasek.

They said the cars did not appear to acknowledge the address from where a command was being sent, only the instruction itself.

"There's no authentication," said Mr Miller.

"But there are restrictions - the car has to operate very fast. If you run into a wall you need to kill the engine immediately, engage the

airbag.

"Car manufacturers don't have the luxury PC software makers have - if something doesn't work in a car that can't happen, it needs to function."

Mr Miller and Mr Valasek intend to make their research openly available following the conference.

"The information will be released to everyone. If you're just relying on the fact people aren't talking about the problem to stay safe, you're not really dealing with the problem," said Mr Miller.

The hackers set the speedometer to read 199 miles per hour while the car was stationary

Toyota said it invested heavily in security research.

"Our focus, and that of the entire automotive industry, is to prevent hacking into a vehicle's by-wire control system from a remote/wireless device outside of the vehicle.

"Toyota has developed very strict and effective firewall technology against such remote and wireless services. We continue to try to hack our systems and have a considerable investment in state of the art electro-magnetic R&D facilities.

"We believe our systems are robust and secure."

Ford also told the BBC the company takes electronic security seriously.

"This particular attack was not performed remotely over-the-air, but as a highly aggressive direct physical manipulation of one vehicle over an elongated period of time, which would not be a risk to customers on any mass level," it said in a statement.

"The safety, privacy, and security of our customers is and always will be paramount."

"Scary"

Security expert Prof Alan Woodward, Chief Technology Officer at

consultancy Charteris, said that car hacking hasn't been widely discussed because as yet there has been no criminal incident of it.

"I think [car hacking] is one of the most scary things out there - [the hacking of] cars and medical devices are the two things nobody talks about," he told the BBC.

"You've heard of ransomware - imagine that happening inside a car. It won't take criminals that long."

Ransomware is a computer virus that freezes a victim's computer or threatens to release personal files unless a payment is made.

A car crash caused by a hacked car featured as a storyline on the US TV series Homeland but was widely dismissed as fantasy, he added.

"There was loads of talk afterwards saying it was rubbish. I remember saying on Twitter, 'I'm sorry, it's not.'"

However both the researchers and Prof Woodward agree that hacking into a car is not easy.

"This is a very technical attack, it requires a great deal of technical knowledge," Prof Woodward said.

Actor Damian Lewis stars in Homeland, a TV series which featured a car hack storyline

"A lot of manufacturers are doing work on security software but they don't talk about it. It's not about anti-malware software, it's more about penetration testing - finding any holes left in the system.

"When people build things based on software, it is built with Intention A. They never think about intention B - which could be all sorts of nefarious purposes."