BBC

Car hack uses digital-radio broadcasts to seize control

By Chris Vallance
BBC Radio 4

57 minutes ago | Technology

Car infotainment systems can allow drivers to see vehicle status updates, play music and videos, view maps and in some cases run third-party apps

Several car infotainment systems are vulnerable to a hack attack that could potentially put lives at risk, a leading security company has said.

NCC Group said the exploit could be used to seize control of a vehicle's brakes and other critical systems.

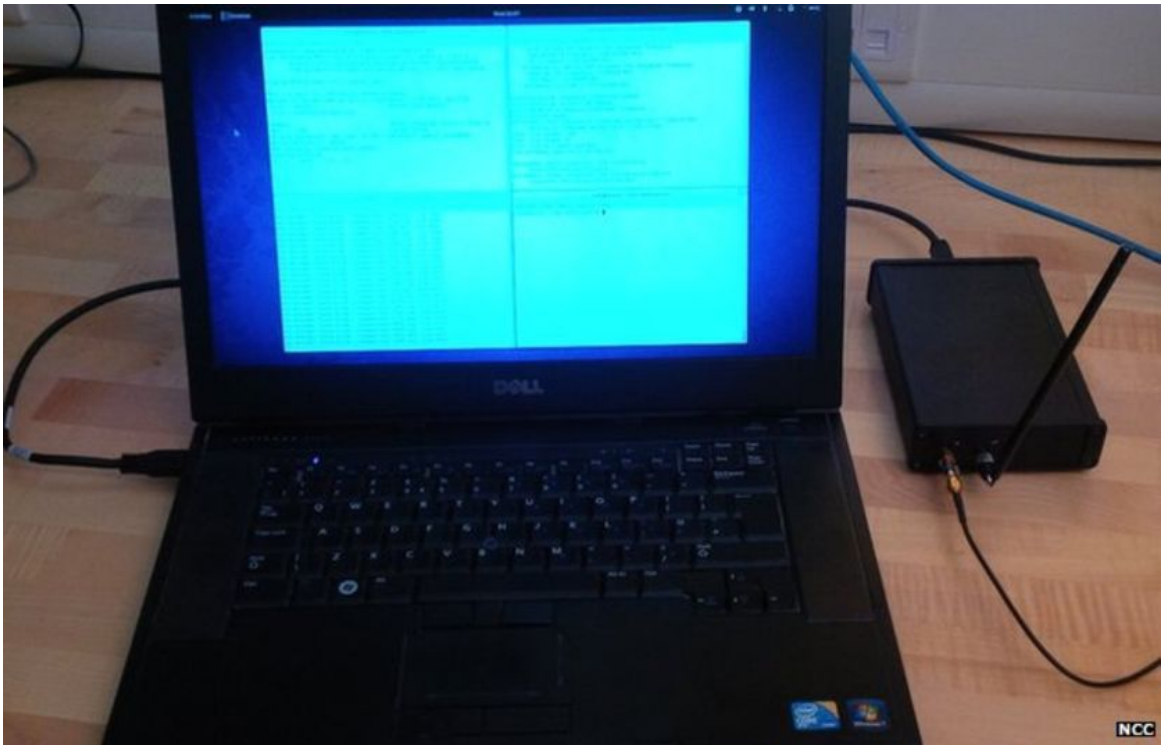
The Manchester-based company told the BBC it had found a way to carry out the attacks by sending data via digital audio broadcasting (DAB) radio signals.

It coincides with news of a similar flaw discovered by two US researchers.

Chris Valasek and Charlie Miller **showed Wired magazine that they could take control of a Jeep Cherokee** car by sending data to its internet-connected entertainment and navigation system via a mobile-phone network.

Chrysler has released a **patch to address the problem**.

However, NCC's work - which has been restricted to its labs - points to a wider problem.



NCC Group was able to transmit the DAB signal using a laptop and a box made from easy-to-source parts

The UK's Society of Motor Manufacturers and Traders has responded by saying that car companies "invest billions of pounds to keep vehicles secure as possible".

Breached brakes

NCC demonstrated its technique to BBC Radio 4's PM programme at its offices in Cheltenham.

By using relatively cheap off-the-shelf components connected to a laptop, the company's research director, Andy Davis, created a DAB station.

Because infotainment systems processed DAB data to display text and pictures on car dashboard screens, he said, an attacker could send code that would let them take over the system.

Once an infotainment system had been compromised, he said, an attacker could use it as a way to control more critical systems, including steering and breaking.

Depending on the power of the transmitter, he said, a DAB broadcast could allow attackers to affect many cars at once.

"As this is a broadcast medium, if you had a vulnerability within a certain infotainment system in a certain manufacturer's vehicle, by sending one stream of data, you could attack many cars simultaneously," he said.

"[An attacker] would probably choose a common radio station to broadcast over the top of to make sure they reached the maximum number of target vehicles."

Mr Davis declined to publicly identify which specific infotainment systems he had hacked, at this point.

Lab simulation

In many ways, modern cars are computer networks on wheels.

Mike Parris, of SBD, another company that specialises in vehicle security, said modern cars typically contained 50 interlinked computers running more than 50 million lines of code.

By contrast, he said, a modern airliner "has around 14 million lines of code".

The addition of automated car controls are creating new opportunities for hackers

Such technology allows the latest cars to carry out automatic manoeuvres. For example, a driver can make their vehicle parallel park at the touch of a button.

Mr Davis said he had simulated his DAB-based attack only on equipment in his company's buildings because it would be illegal and unsafe to do so in the outside world.

But he added that he had previously compromised a real vehicle's automatic-braking system - designed to prevent it crashing into the car in front - by modifying an infotainment system, and he believed this could be replicated via a DAB broadcast.

"If someone were able to compromise the infotainment system, because of the architecture of its vehicle network, they would in some cases be able to disable the automatic breaking functionality," he said.

Jeep attack

On Tuesday, Wired magazine reported that two US security researchers had managed to remotely take control of a Jeep Cherokee's air-conditioning system, radio and windshield wipers while its journalist was driving the vehicle.

Wired magazine reported that a Jeep Cherokee had been hacked

Mr Valasek - director of vehicle security research at IOActive - said that NCC's attack appeared to have similarities with his own.

"I mean that's essentially what we did over the cell [mobile] network - we took over the infotainment system and from there reprogrammed certain pieces of the vehicle so we could send control commands," he said.

"So, it sounds entirely plausible."

But he added that such exploits were beyond the reach of most criminals.

"It takes a lot of time skill and money," he said.

"That isn't to say that there aren't large organisations interested in it."

More details about both the NCC and the US team's research will be presented to the Black Hat security convention in Las Vegas next month.