Hacking sends shivers through brave new world of digital cars

September 18 2015, by Romain Fonsegrives

High-tech electric car maker Tesla has recruited talent to protect against cyber attacks

The connected car may be catching everyone's imagination at this year's IAA auto show. But the new technology also brings with it new dangers, such as hacking.

Carmakers at the Frankfurt Motor Show, which opens its doors to the

general public on Saturday, are keen to show off their brave new world of intelligent, digitized models.

But an incident in the US earlier this year when computer hackers remotely took control of a Jeep Grand Cherokee while it was driving on a motorway and brought it to a standstill highlighted the dangers that such innovations can bring.

And the industry must find ways of convincing consumers that these new super-computers on wheels are safe and secure.

One Jeep owner, Michael Frosch, is taking an extra close look at different models on display at the IAA.

"I have the same navigation system as in the Jeep that was hacked," he says.

"But I guess I'm not important enough for someone to want to send me crashing into a tree."

Jeep was forced to recall 1.4 million vehicles in the US in the wake of the hacking incident, which was a real wake-up call to the potential dangers, says Ricardo Reyes, vice president of US startup Tesla, a maker of upscale electric cars.

"We were mobilized before" the incident with the Jeep, but "awareness is much stronger" now, says Brigitte Courtehoux, director of PSA Peugeot Citroen's connected services business unit.

German auto giant Volkswagen has promised to turn "all of our models into smartphones on wheels" by 2020.

But as was the case with computers and mobile phones before them, that

will make cars potential targets for hackers.

Around 150 million connected cars will be on the road worldwide in 2020, according to estimates by consultancy firm Gartner.

Fiat Chrysler Automobiles issued a safety recall for 1.4 million US cars and trucks in July after hackers demonstrated they could remotely control their systems while the vehicles are in operation

For the time being, "there is no clear economic model for hacking cars. But once your car stores sensitive data, that will start attracting criminals," said Egil Juliussen, analyst at IHS.

And those criminals always keep pace with any technological advance.

"A connected car is only secure for a short time" until a chink in the armour can be found, said Andrey Nikishin, director of futures technologies projects at the cybersecurity consultants Kaspersky.

'No big challenge'

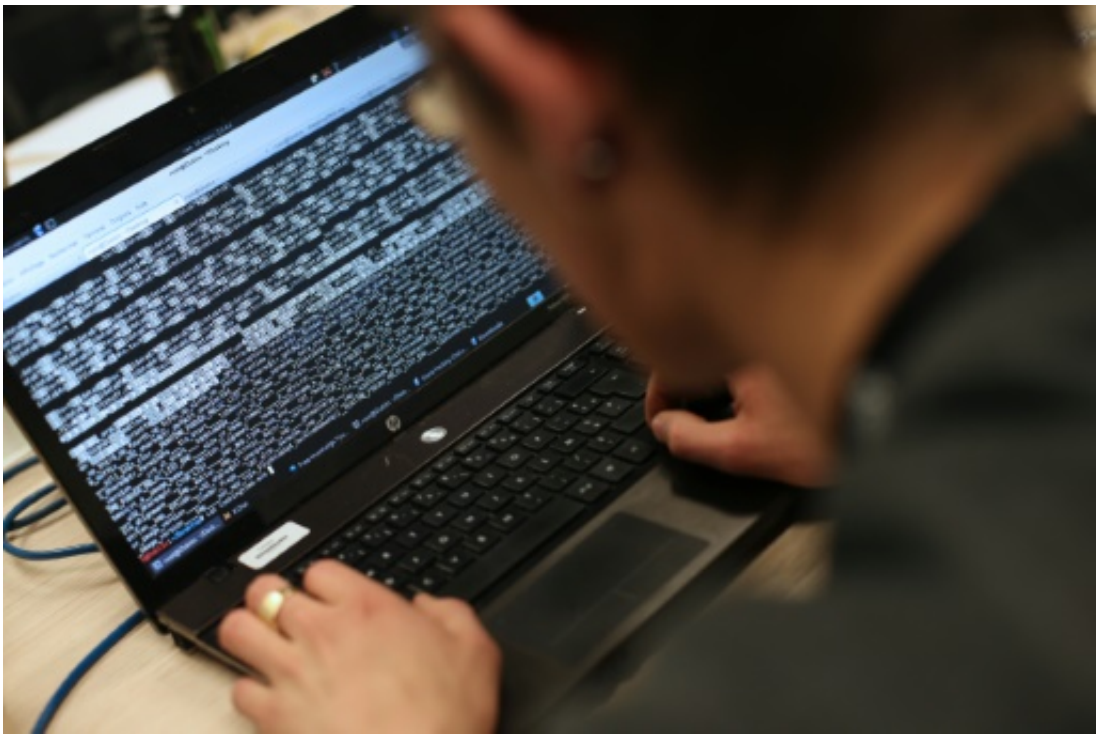
At the moment, "it's not really easy to hack just any car on the road. But for a professional hacker with lots of time on their hands, it is no big challenge," Nikishin said.

In London, for example, around 6,000 cars were stolen in 2014 without being broken into, but simply by hacking their electronic locks, according to the city's police.

But theft or accidents are not the biggest threats, Nikishin said.

Protecting personal data "is the most pressing problem because it's a lot easier to steal the data," the expert said.

For example, such a risk could arise if connected cars are synchronised with drivers' smartphones containing personal credit card or bank account details.



A virus called "CoinVault", which first appeared in May 2014, managed to lock some 1,500 computers, all of which used the Windows operating system

And while "hackers" currently tend to be well-intentioned researchers, the weak points can quickly fall into criminal hands, said Juliussen.

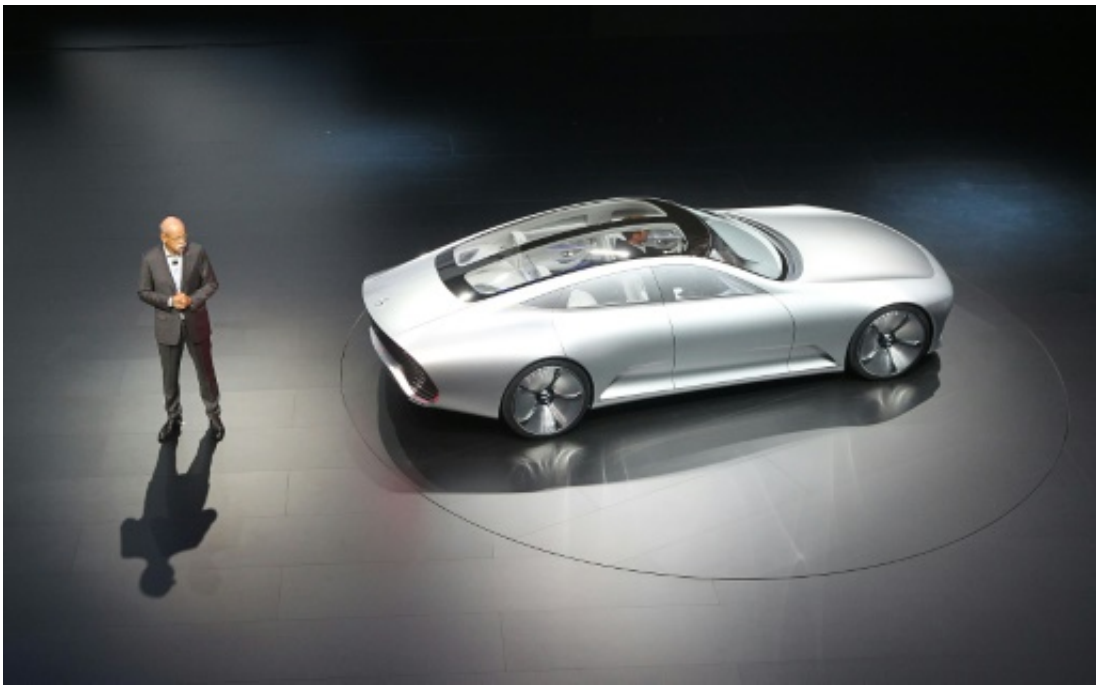
At the IAA, the European Automobile Manufacturers' Association ACEA outlined its "principles of data protection in relation to connected vehicles and services."

"Data protection is an issue automakers take very seriously, as we are committed to providing our customers with a high level of protection and maintaining their trust," said ACEA chief, Carlos Ghosn, who heads French carmaker Renault.

Nevertheless, the industry is not always moving at the same pace on the

matter.

German automaker Daimler and its chief executive Dieter Zetsche, for example, boast that data collected by the group is stored on its own secure servers, rather than those of third parties, contrary to some of its rivals.



German automaker Daimler and its chief executive Dieter Zetsche have said that data collected by the group is stored on its own secure servers, rather than those of third parties, contrary to some of its rivals

PSA Peugeot Citroen is collaborating with IT giants such as Cisco on an electronic architecture for its cars, as well as "some players from the military sector," says Courtehoux.

US manufacturer Tesla is taking the bull by its horns and working

together with hackers themselves.

And the IT sector is also taking the dangers seriously. This week, US giant Intel set up a new research group, the Automotive Security Review Board, to look into ways of reducing the risks of connected car hacking.

In Germany, Volkswagen announced a similar cybersecurity research project with insurer Allianz, and chemicals giants BASF and Bayer.