Article presented:
https://cacm.acm.org/news/257247-car-hackers-could-drive-you-off-the-road-or-they-might-settle-for-money/fulltext

Article presentation

This article is focussed on the security problems presented by modern cars.

Modern car, like many other “things” of the internet of “things”, are connected to the internet for multiple reason. As presented in the article, one of theses reason is to automatically bill the charge of an electric car. But, as you can probably guess, there are many other use for internet connection in modern cars, such as downloading updates for the maps of the car navigation system, downloading updates to another component of the car[1], interacting with other cars for better autonomous driving.

Theses connections present a security risk if they aren’t properly secured. The article detail the case of the 2014 “Fiat Chrysler Jeep Cherokee” car, which was sold in the U.S. This car was recalled by the manufacturer, because a security loophole, demonstrated in this video[2], allows for malicious hackers to remote control the car. The video is very impressive.

As explained in the article, it’s easy to perceive the possibility of very dangerous exploitations of such loopholes. For example if a hacker where to get control of the car of a public personality to assassinate them. Even worse, one can imagine a hacker getting control of multiples cars of the same model and disabling a core function, such as the brake. Depending on the popularity of the model this could kill more than 10^4 people.

Benefit of autonomous and connected car

Now, in sheer contrast from the previous paragraph, it is important to remind the reader that autonomous and especially autonomous and connected car have many benefits. The obvious and famous one is to have multiple car connected together so that they can drive in perfect synchronization[3]. Another famous one is that a autonomous car doesn’t need to sleep and doesn’t drink alcohol.

Solution to the problem presented in the article

In my non expert opinion, it is clearly possible to make a perfectly secure and fully connected car.

There are 2 problems that need to be addressed:

-First and most importantly, the car should be connected to the internet as an end device. In other words, it should behave like a smartphone or laptop, which by default are not hosting any servers and therefore have a firewall that blocks any inbound connection, and, to simplify greatly, only accept responses from requests that the device made. I understand that this might sound “naive” and I’m not sure the security problems come from here, but I don’t see how you can enter a device if it doesn’t allow any inbound connection.

- Secondly, I believe that the car industry and society as a whole would gain from standardization of the cars’s interfaces with the outside world. In other, the communications protocol should be standardized. That would provide the benefit of easier interaction between multiple cars and the benefit of a more secure system because it would be designed only once by experts instead of many time by each car manufacturer.

---

[1] such as the “autonomous driving” component

[2] https://www.youtube.com/watch?v=MK0SrxBC1xs

[3] For example, if a car 2km ahead of you sees an accident or a slow down of traffic it would be able to automatically warn you car so that it can stop accelerating at the right time instead of braking in 2km.