Modern cars and their security shenanigans

In the old days when the infotainment panel of a car used to consist of dials and switches, stealing a car used to be quite a straightforward task, pick the door lock (or smash a window) then hotwire the car and you are in. In the modern day however things are not so simple, one doesn't get a singular option of entry point anymore, instead one gets a platter of them.

Most cars these days come with key fobs instead of normal keys. A key fob emulates the role of a key by sending radio signals to a receiver unit (car lock) for the purpose of authentication. This has eliminated hotwiring wholesale and thus made cars more secure, except the fact that it did not. Now thieves don't need to steal your car keys or hurt themselves breaking windows, they just need to replicate the signals generated by it, which they can do easily while being 20 meters away from you.

With key fobs it was just one signal that could be manipulated but with infotainment systems you get wifi, bluetooth… every signal known to mankind that one can make use of to get an access to your car. Once an attacker gets entry to the system, the playing field expands to another level.
With features like lane assist and cruise control the car’s brain can make movements of its own, So when someone gets access to it, they get themselves a real life remote controlled car, and the cherry on top is that this can all be done remotely.

EV public chargers are another entry point which hackers can target to compromise EV security. The average time that an EV spends at a charging station can range from half an hour to a couple of hours, depending on several factors like bowel movement of passengers, their shopaholic nature etc. This time is more than enough to insert malicious software either through the charger to the EV or the other way round, both situations pose risks of colossal nature. The former scenario can lead to the endangerment of lives of hundreds of thousands of people who get their EVs infected from the charger, the latter scenario can lead to the attacker infiltrating the power grid and bringing the entire economy of a country to a standstill. One might think though that this is a good plus point for ICE cars, as they barely have to wait at a petrol station for a couple of minutes so no chance of hacking doing to them right?

In December 2023 70% of petrol pumps across Iran were targeted by a cyber attack which rendered them non functional for quite some time. Transportation services were driven to a halt and thus so was most of the country

In conclusion all kinds of modern vehicles are in the same field when it comes to the aspect of hackability. So what is it that a normal user can do to escape this matrix? regularly updating the car’s software is the best we can do to protect our car, because it's this step that makes sure that the security patches which manufacturers have spent millions of dollars in making, do end up reaching us. Using a metal box to store key fobs is another way to prevent hackers from replicating its signal and thus preventing a trip to the police station.

Another way that the regular public can use to make sure a more secure (less hackable) automotive industry is to pester manufacturers for more pentesting and bug bounty programs. In such events skilled hackers are allowed to compete against one another in finding and exploiting bugs in a given software, under strict time constraints for cash rewards. Such events have proven time and again that they are extremely productive in making softwares more secure.

The 2024 pwn2Own automotive event hosted in Tokyo is just an example. In this event a team called “Synactive” hacked Tesla twice using 49 zero day exploits (unknown security flaws). Tesla was then given 90 days to fix those bugs before they were published and that’s just as productive as it gets.

Let's say though at some point the ball does get rolling towards massive security advancements, then does that mean vehicles will become impossible to be hacked? No.

That is the answer that almost all cyber security professionals would give you. No matter how much energy you invest in large scale security advancements you cannot achieve a 0% hackability chance and if you do then it's a delusion. The very system you create to defend you can be used to attack you, take AI for an example.

What is the point of it all then you might wonder, well it is to reduce the chance from 1 in 10 to 1 in a million to 1 in a billion, that there will be an attack for an attack there will be.

.