Automobile Security

Cars are computers on wheels. Let's take a look back into the history of automobiles. We disregard the part where the interaction with components inside the car was purely mechanical. At one point, car manufacturers added *electronic control units (ECUs)* that manage everything from engine performance to entertainment systems. ECUs are special embedded devices, therefore have a processor and memory, which react to sensor inputs to make decisions [1]. However, they need a means of communication. Either, one could wire up every control unit with every dependable control unit or come up with a unified approach to let components communicate. The *Controller Area Network (CAN)* was born in 1986 by the German car component supplier *Bosch*. The general idea behind CAN was to create a standardized method for ECUs to communicate in real-time without requiring a host computer by broadcasting messages to each ECU which then can decide if the message is intended for them. Furthermore, message have no source or destination identifier [1].
CAN is safe. ... as long as it is a closed network. The threat modelling back then did not assume that cars will be exposed to other networks or that a none critical component could access the CAN-bus. At that time, the most important design aspect was availability for safety concerns. If I hit the break, I certainly want the car to stop over everything else. However, Car manufacturers kept pushing for new features like movies, traffic assistance or even autonomous driving. For example, carmaker *Ford* submitted a patent request to let a car drive back by itself to a defined location if the owner misses payments [4]. Due to the nature of CAN, having access to the network means that we can easily inject messages and sniff messages [1].

This screams that cars will become heavily connected devices as time progress which will communicate with the outside world. Obviously, this has many advantages in terms of innovation. On the other hand, this opens up the gates for a broader attack surface. Many systems communicate remotely [2]:

- The *Tire Pressure Monitoring System* is inside the tire and communicates via radio frequencies with a range of up to 1 meter
- The *Remote Keyless Entry* to unlock a car can result in a denial of driving if attacked because of it long range of up to 20 meters
- Telematics, Cellular, Wi-Fi which can have high ranges dubbed the *holy grail of automotive attacks*

Remote C(ar)ode Execution. Before enumerating different existing attacks, I want to highlight the work of *Dr. Charlie Miller and Chris Valasek* who hacked a Jeep back in 2015. They open sourced a remarkable collection of intelligence about car hacking.

- Researcher conduct an experimental analysis of car security with driving disabled car attaching wires to a debug port to listen to CAN messages. This work was one of the first glimps into what an attacker can do if she has access to the CAN bus. They were able to take control of the brake without the possibility of a manual override of the driver [5]
- While a reporter was sitting inside a Jeep, it was fully controlled by remotely stopping the reporter on a highway at the end [3]
- A vulnerability in the Wi-Fi firmware allowed attacker to abuse a heap overflow resulting into remote code execution on a *Tesla Model S/X* [6]

Summary. Summa summarum, car security is an increasingly worrying field with new features added to cars to connect them to networks and maybe other driving participants in the future. This is a prime example where cyber security is directly associated with human safety. The attacks enumerated could directly impact human lives - remotely killing someone by letting it look like an accident with emergency brakes which can not be manually overridden. Also, cars are produced *en masse* and have a great longevity of up to 10 years! Manufacturers have to provide updates for cars that are even 10 years old. It's quite the opposite for mobile phones, where each new generation a new one becomes obsolete and therefore doesn't receive software updates. For example, when the car has its annual safety inspections, a check for security like 'up to date' software should be included as well. Someone could argue that carmakers should also be responsible to provide 'state of the art' security which would push cars into a subscription based service. Let's see how carmakers will deal with subscription of services in the future, like *Mercedes does with a faster acceleration paywall* [7].

References

[1] Chris Valasek Dr. Charlie Miller. Adventures in automotive networks and control units. https://illmatics.com/car_hacking.pdf.

[2] Chris Valasek Dr. Charlie Miller. A survey of remote automotive attack surfaces. https://illmatics.com/remote%20attack%20surfaces.pdf.

[3] Andy Greenberg. Hackers remotely kill a jeep on a highway — wired. https://www.youtube.com/watch?v=MK0SrxBC1xs.

[4] Sarah Jackson. Ford wants to allow your car to lock you out — and even drive itself to an impound lot or scrapyard — if you miss payments. https://www.businessinsider.com/ford-patent-cars-repossess-themselves-drive-away-if-missing-payments-2023-2.

[5] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy*, pages 447–462, 2010.

[6] Tencent Keen Security Lab. Exploiting wi-fi stack on tesla model s. https://keenlab.tencent.com/en/2020/01/02/exploiting-wifi-stack-on-tesla-model-s/.

[7] By Jess Weatherbed. Mercedes locks faster acceleration behind a $ 1,200 annual paywall. https://www.theverge.com/2022/11/23/23474969/mercedes-car-subscription-faster-acceleration-feature-price.