Hi Iason, it was very much insightful reading your post, to take this further, let’s discuss a couple attack vectors on autonomous vehicles; such as hacking into the vehicle telematics, or into the sensors.

Considering a scenario where in the near future, a self-driving vehicle's telematics unit may need a modest upgrade. The device that receives and installs this patch might be immediately linked to the vehicle's network, with the existing hardware initiating the process once the vehicle is parked. Imagine one of these receiving devices sharing a CPU with a standard smart device that ambitious hackers might penetrate and unlock, meaning that this device could be abused to replace manufacturer updates with user-generated ones. A competent attacker might potentially install ransomware on tens of thousands of automobiles, providing the power to lock out users or freeze vehicles until the owners pay a ransom. Manufacturers would struggle to prevent the assault, since their exclusive maintenance channel would be blocked, and owners could not even guide their cars to a repair facility.

The other scenario where the sensors could be hijacked laterally, at the junction of critical and noncritical vehicle buses, a message injector may be able to send undesired data to car electronics. The electronics that regulate cabin lights and play music should theoretically be impossible to connect with systems that conduct crucial functions such as braking and acceleration. At present, these car networks are physically linked at the telematics or body controller units, enabling data to propagate across networks.

**References**

* Nash, L., Boehmer, G., Wireman, M. and Hillaker, A. (n.d.). Securing the future of mobility Addressing cyber risk in self-driving cars and beyond. [online] Deloitte. Available at: https://www2.deloitte.com/content/dam/Deloitte/be/Documents/strategy/Securing%20The%20Future%20Of%20Mobility.pdf [Accessed 17 Sep. 2022].