Lack of cyber security poses threat to modern cars

January 31 2017

Credit: AI-generated image (disclaimer)

Cars are becoming increasingly smarter and are connected with each other and their surroundings to an increasing extent via their on-board systems. From April 2018, it will be mandatory for all new cars manufactured in the EU to be connected via eCall (emergency call). However, these mobile computers are not designed to keep malicious

hackers at bay. The automotive industry needs to take the lead in order to improve cyber security. This is the conclusion of Hebert Leenstra derived from his research into the automotive industry conducted at the Cyber Security Academy in The Hague. Herbert Leenstra believes that it is high time for a complete overhaul of the ICT architecture in cars to ensure that consumer safety is guaranteed.

Connected

Connected cars, including self-driving cars, are in constant communication with their surroundings. All modern cars are fitted with microchips featuring software that controls various functions of the car, such as engine management, navigation and the entertainment system. This software uses Bluetooth, WiFi, 4G/5G or satellites to communicate with other cars and networks. Herbert Leenstra explained, 'It is fairly easy to gain access to the vehicle's CAN bus using the internet. The CAN bus is where all of the ICT systems come together, essentially the car's cyber backbone. This is where you can adjust all the car's settings, so hackers who gain access can directly influence the car's safety devices. In 2015, hackers successfully gained access to an American Jeep Cherokee while it was on the road. They were able to jam the brakes and adjust the speed of the vehicle.'

Fundamental flaws

The research found fundamental flaws in the ICT architecture of the current generation of vehicles. Leenstra clarified, 'The research shows that there are various ways for hackers to access the car's ICT system. For example, the entertainment system currently grants access to the engine system, while there is actually no plausible reason for these two systems to be linked. Now that the current generation of cars is connected to the internet, hackers can also use the internet to hack

various car systems.'

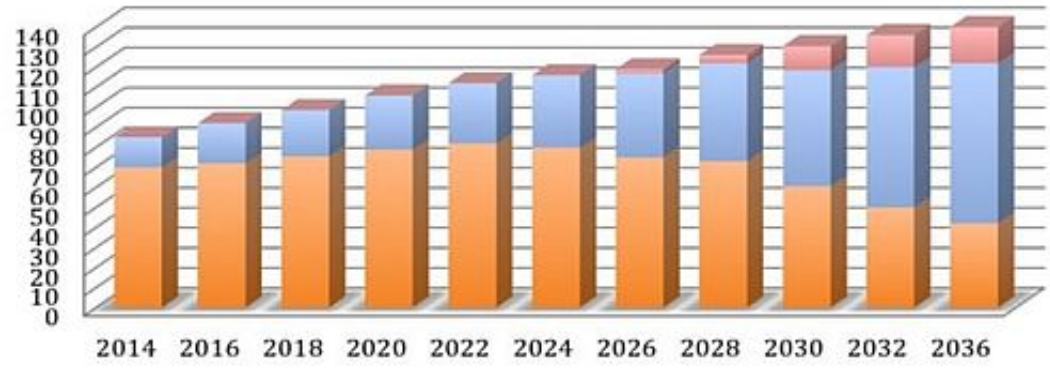

Fig. 3. Global Market for cars in mln, Traditional driven car, Semi-autonomous car, Autonomous car [12]

Updates

The research has resulted in concrete steps being identified, which the various parties in the automotive sector can take to improve cyber security in cars. Leenstra added, 'Firstly, car manufacturers need to redesign the current CAN bus system in their cars so that the car's essential and non-essential systems are separated. This would make them less susceptible to hacking. Secondly, the government needs to offer confirmation on several fundamental principles, so that the automotive industry is able to build upon solid foundations. For example, the industry is awaiting answers on subjects including the length of time that car manufacturers are required to support car software updates, security patches and firmware updates. Another question concerns how the updates should be implemented. Such an update could proceed via a USB stick or via the internet, but a USB stick can naturally hold all sorts of information.'

Safety

Leenstra also thinks that improvements could be made regarding the role played by insurers, sharing information about incidents and expertise on cyber security. Leenstra clarified, 'Europe could follow America's lead and establish a car Information Sharing and Analysis Center (ISAC). Within an ISAC, all involved parties share their information and experiences regarding security.' And the consumer? 'Consumers should be sure to ask their dealer critical questions about how cyber secure the car is, and how the manufacturer can prove the car's credentials.'

More information: Multi-actor roadmap to improve cybersecurity of consumer-used connected cars. www.tbm.tudelft.nl/fileadmin/F … inal-v11-01-2017.pdf

Provided by Delft University of Technology