Anorectics for Hackers

It is still mostly the "good" hackers who use networked cars as targets for cyber attacks. Not infrequently, the automotive industry even uses them to develop security solutions for mobile software with a network connection. One example is a cross-industry partnership between T-Systems and Argus Cyber Security.

COPY —— Roger Homrich

Whether at Volkswagen or Toyota, Volvo or Peugeot – vehicles that roll off the manufacturers' production lines today have around 100 million lines of programming code, seven times as much as a Boeing 787. So the car is a moving computer – and just like a computer, it can be hacked. Autonomous cars will offer a lot of potential for attacks. They could become fat prey for hackers. Because the networked car is a real data oasis for them. On average, we spend more than four years of our lives in a car. And during this time we are increasingly using it as an exchange platform for data – consciously or unconsciously. Even the current models are constantly exchanging information with the outside world. If attackers succeed in manipulating this data traffic or changing software, it becomes dangerous.

STEERING WITH THE ACCELERATOR PEDAL

Stefan Nürnberger, computer scientist and IT security expert at the Helmholtz Center for Information Security (CISPA) in Saarbrücken, has already hacked many cars. Searching for gaps in their IT infrastructure, the white-hat hacker often succeeds in attacking via faulty radio connections. If, for example, Bluetooth is not programmed correctly, malware can be smuggled in via a smartphone and the software in the car can be manipulated. At the simulator it can also become dangerous if the driver steers the car with the accelerator pedal after an intervention in the electronics.

Horror messages from hacked cars are still rare and "good" hackers usually reveal the weak points on behalf of car manufacturers or out of pure curiosity. The hacker, who calls himself L&M, demonstrated to the US tech magazine Motherboard at the end of April this year that he had broken into about 27,000 user accounts of two GPS tracker apps. This would not only have allowed him to determine the current position of the vehicles. Regarding some of the cars, it would even have been possible to switch off the engine remotely while driving up to a speed of 12 mph.

GOVWARE FOR CARS

Also for police and secret services the car seems to be a rich source for search and reconnaissance. The Central Office for Information Technology in the Security Sector (ZITiS), for example, wants to gain access to the car and use govware for this purpose. In March 2019, at the request of a member of the German Bundestag, the Ministry of the Interior replied: "The development of forensic investigation capabilities for connected cars and the provision of corresponding capacities are included in the fulfilment of ZITiS' tasks".

In any case, car manufacturers and suppliers are upgrading their IT security systems. Continental, for example. One of the world's largest automotive suppliers is now pre-integrating security solutions from Israeli security pioneer Argus Cyber Security into the networked electronic components in automobiles. Argus has been part of the Continental subsidiary Elektrobit (EB) since 2017. Its embedded software solutions are already installed in more than a billion vehicles worldwide.

Together, EB and Argus offer multi-layered, end-to-end cyber security solutions and services to protect networked vehicles from cyber attacks. With solutions to protect individual electronic control units (ECUs) or the vehicle network. In addition, they enable mobile software updates with an over-the-air solution. T-Systems and Argus are pooling their security know-how in an industry-wide partnership. They are setting up an Automotive Security Operation Center to complement Argus' in-car security solutions and protect networked cars from cyber attacks in real time.

Photo: Continental AG

Maximum frustration for hackers

External Interface Protection & Monitoring
In-Vehicle Network Protection & Monitoring
In-Vehicle State-of-Health-Monitoring
Security Field Monitoring
Over-the-Air Software- and In-Vehicle Update

Yoni Heilbronn, Vice President Marketing at Argus, on weaknesses in the car and the fight against car hackers.

The protection of networked cars is complex because, in addition to the software in the car, networking offers further points of attack. This is how the car develops into a mobile data center. What is Argus' defense strategy?

Nobody in the security market offers THE magic bullet to get all risks under control. IT security for the car will always remain a challenge, as there will be no 100 percent security against cyber attacks in the future. We can only try to get as close as possible to this optimum. To do this, we have to look at the vehicle at different levels, for example the software of the control elements or the networking of terminal devices with the vehicle via Bluetooth or, in future, the entire car via 5G. We have to make each of these levels as safe as possible. If a hacker then attempts an attack, we make life so difficult for him that he hopefully gives up his attack. So we have to frustrate him as much as possible.

What are the solutions for each level?

Our multi-layered approach corresponds to an end-to-end offering for automotive cyber security, ranging from the development of new products to ongoing monitoring and the ability to fix vulnerabilities through over-the-air updates. It starts with the ECUs and software in the car. The software should not contain errors that could be exploited by attackers. This is not self-evident. Software contains an average of seven errors per 1,000 lines of code. Today we have up to 150 million lines of code in one vehicle. So a car leaves the factory with thousands of known errors. And there are experts who say that there are another 50,000 unknown errors. Of course, not all of them open the doors to the vehicle for hackers. But we have to be able to develop error-free software.

But software of individual control elements in a car does not work independently of each other.

It gets even more complicated because the controls and software come from several suppliers. It all comes together in one car. That's why we also have to protect the router as a gateway within the vehicle network. It integrates our safety functions and provides basic vehicle diagnostics and over-the-air software updates to monitor the vehicle's cyber-health and perform immediate necessary updates. There is an in-vehicle server for server-based architectures in the vehicle. This is a high-performance computer that acts as a network manager and communication interface.

What makes it so difficult to protect networked cars?

Everything that is networked has some interface to the Internet and can be attacked from outside. That was not the case until now. Although the car has been a rolling server for many years, it had no door to the outside world. So anyone who wanted to manipulate had to get directly into the car. But what was possible, for example with rental vehicles.

Two examples: Older cars transmit the tire pressure via a Bluetooth interface. This interface can be used to install malicious code. Viruses can also be smuggled in via USB ports and CD drives. Hackers, however, are usually located somewhere in the world. The car was therefore not an attractive target for them. Now every car is somehow networked: via a passenger smartphone, the navigation system or, in Europe, the eCall. Now malware can be sent into the car. The art now is to not only harden software in the car against attacks. Rather, attacks must be detected in real time so that we can react to them. This is exactly what we do with Automotive SOC and Security Information and Event Management (SIEM): real-time analysis. We can then initiate countermeasures, for example with software updates. Car manufacturers and fleet operators can then import this update into any vehicle on a mobile basis.

Michael.Jochum@t-systems.com
www.t-systems.com/telekom/auto-soc
www.t-systems.com/white-paper/auto-soc