Protecting the connected car against cyberattacks

By Timo van Roermund, NXP

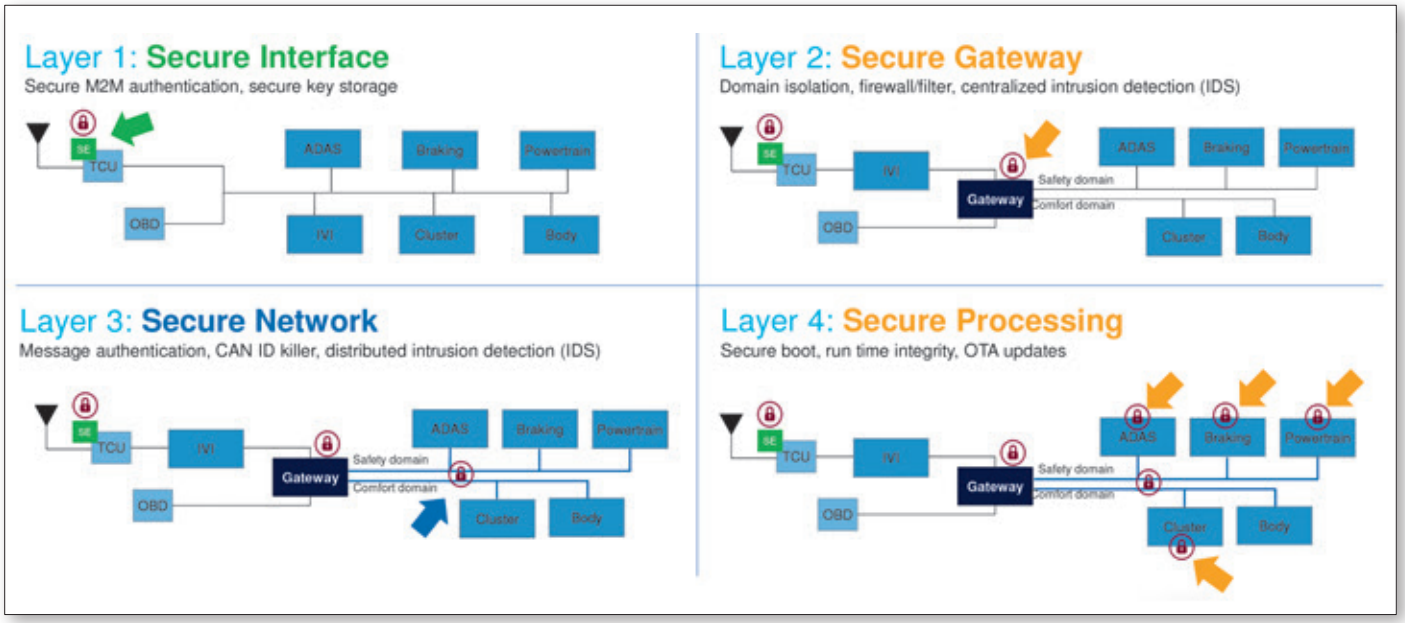
This article highlights how secure interfaces, secure gateway, secure network and secure processing can protect the connected car against cyberattacks, and allow its users to be in full control of their data, making the connected car an opportunity for business and society, rather than a threat to us all.

The automotive industry is rapidly evolving and the car is being transformed from a simple mode of transport to a personalized mobile information hub. All these electronic functions bring great benefits to the driver, increasing comfort, convenience, safety and efficiency. But these features come with new risks, too. Modern vehicles are gradually turning into smartphones-on-wheels, which continuously generate, process, exchange and store large amounts of data. Their wireless interfaces connect the in-vehicle systems of these connected cars to external networks such as the internet, enhancing consumer experience by enabling new features and services. But this connectivity also makes the connected car vulnerable to hackers who attack the vehicle by seeking and exploiting weaknesses in its computer systems or networks. In fact, recently hackers indeed demonstrated that they could gain remote control over vehicles.

Until recently, cars have been isolated from their environment and from the internet. The only exception was maybe the interface for vehicle diagnostics, but because this OBD-II port is a wired interface, it could rely on the physical protection offered by the vehicle chassis, like the electronic control units (ECUs) and the in-vehicle network (IVN). But things are changing rapidly, most modern cars already allow smartphones to be paired via Bluetooth with the car radio for hands-free phone calls or to play music. And it doesn't stop there: many modern cars are wirelessly connected to the internet, for example to enable additional services in the car and, to a certain extent, provide for remote control over the car such as remote unlocking and starting. Their wireless interfaces connect the in-vehicle systems of these connected cars to external networks such as the internet, which forms an entry point for hackers, opening the door for remote attacks.

The range of attacks that a connected car faces is extensive and diverse: it varies from relatively simple attacks, in which for example malicious messages are sent to a vehicle, to more sophisticated attacks in which hackers may open up ECUs and try to reverse engineer their microcontrollers and software. Cyberattacks pose a threat to the reliability and safety of the car: the hacker can potentially take control over the car, as well as to the privacy of the driver, and the vehicle data can be used to build a profile of its user(s). Therefore, steps need to be taken now: the connected car must be secured, to ensure the correct functioning of all in-vehicle systems, as well as user privacy. This implies a paradigm shift in the design of in-vehicle electronics. A first reason for that is there isn't a single, well-defined hacker. In fact, there are various attackers, with different motivations, skill levels and resources. For example, there may be (academic) researchers who try to take (partial) control over the vehicle, for scientific reasons. Or there may be (organized) criminals with large budgets that want to steal valuable data from a vehicle, for financial gain. Traditionally, there has been a strong focus on safety, meaning that for example the brakes should function correctly under all circumstances. Safety will remain equally important in the future, but the increasing amount of electronics and software in vehicles will additionally require security, to protect the vehicle against hackers.

In 2015, vehicle hacks reached the popular press, with the Jeep and Tesla, and caused some of the biggest vehicle recalls in history. For the first time, the public started to understand the need for increased in-vehicle security. US politicians felt the need to get involved and most recently the FBI have decided the risk is so high, they have even issued warnings to the public. But the events of last year have also shown the world that different OEMs had different security levels in place already, and different speeds of solving the issue. Most vehicle hacks consists of a number of smaller steps. It usually starts with finding vulnerability (a bug) in a system that is remotely accessible. But once you get for example into a car



The four layers of automotive security

telematics unit, you have a good chance of getting into just about any other part of the car such as the ECUs that control engine speed, braking, cruise control, valet parking etc. It is good practice to use multiple security techniques to mitigate the risk of one component of the defense being compromised or circumvented. Implementing a framework of 4 security layers will lead to a highly secure vehicle network:

To secure the connected car, one has to start with the external interfaces themselves. First of all, the communication channels need to be protected against data theft, e.g. by encrypting the data, and against manipulation, e.g. by authenticating the messages that are exchanged to protect their authenticity and integrity. Furthermore, the interfaces need to prevent unauthorized access. This involves processes such as machine-to-machine authentication to check that you are communicating with a known or authorized device.

As we saw with last year's Jeep hack, once hackers obtain access to a network, they can send messages anywhere. This is where layer 2, the secure gateway, plays its part. A central gateway ECU separates the TCU and OBD from the network and breaks up the vehicle network into functional domains, with the gateway firewall deciding what nodes can legitimately communicate with other nodes. In the Tesla Model S hack of 2015, the protection offered by the gateway was highlighted as a key security feature for modern vehicles. In the Jeep hack, hackers could switch off brakes remotely due to the lack of a gateway. In the Tesla hack, the worst they could do was sound the horn! Apart from isolation, the most important function of the secure gateway is the firewall that separates the external interfaces from the safety-critical inner vehicle network. The gateway engine is a contextually aware routing function that determines, by a number of increasingly sophisticated checks, which messages are currently legitimate, and will pass through the gateway onto the destination.

Securing the interfaces is a critical requirement, but on its own may not be enough to stop hackers. For example, they could compromise and impersonate a trusted device and use this to bypass access control. Therefore, one has to apply additional lines of defense. One logical place to do so is in the in-vehicle network, which forms the spine of the vehicle and connects all the different parts of the brains (ECUs). For example, countermeasures may need to be implemented on the network level. Once the external interfaces and internal networks are secured, the brains of the connected car must also be protected. These brains are formed by up to (and in some cases, over) a hundred individual computers (ECUs) that together implement the control functions in the car, including many advanced (automated) driving functions. These ECUs continuously generate, process, exchange and store large amounts of valuable (sensitive) data. And this protection helps in different ways.

1) Prevention of access, e.g. using machine-to-machine authentication and gateway firewalls, to ensure that hackers cannot access and tamper with the safety critical nodes in the vehicle.
2) Detection, e.g. secure boot of the controller, to validate that the software is genuine and trusted.
3) Reduction of impact, e.g. by isolating the network domains, to prevent a compromised infotainment unit being used to control e.g. the brakes.
4) Fixing vulnerabilities e.g. enable full vehicle OTA update capability through the secure gateway, to fix vulnerabilities before they can be exploited (at large scale) by hackers. The connected car, as part of a smarter world, is highly connected and constantly interacting with its environment. In a new era of vehicle complexity and connectivity, these connections bring enormous promises for increased comfort, safety and efficiency. But with that there opens a new era of ingenuity and resourcefulness for car hackers, as with all connected devices, and the connected car becomes a target for cyberattacks. The security of the vehicle electrical architecture is vital to ensure the safety of the vehicle occupants. To secure all of this, an integral approach is needed where countermeasures are applied at all levels. The exact security requirements for a specific vehicle need to be determined using a thorough risk analysis that must be part of its design process. ■