'Hello car, what is the password?'

March 1 2013

Credit: AI-generated image (disclaimer)

As cars get clever - bristling with computer chips and networking capabilities - an EU-funded project makes sure that your car's data stays safe and the networks are secure from hackers and tampering.

If you ever wanted proof that we live in a computerised, data-hungry and networked world, just disassemble your car. There is more gadgetry, electronics and microprocessing power on board an average car than

most people would ever image. All over the vehicle sensors gather information on engine performance, wear and tear, oil quality and tyre pressure. They can detect the first signs of a skid or roll and activate emergency systems such as electronic stability control.

'To improve traffic safety and traffic flow, many companies and research organisations are investing a lot of effort into ground-breaking research to develop vehicle communication and networking systems,' explains Olaf Henniger from the Fraunhofer Institute for Secure Information Technology. 'Europe is really forging ahead in car-to-car and car-to-infrastructure networking.'

Car-to-car (C2C) communication allows vehicles to 'talk' to each other to share information, perhaps about congestion on the roads or indicating their presence in fog or around blind corners. Car-to-infrastructure (C2I) communication lets vehicles connect with traffic lights, or other road infrastructure, which can help to optimise traffic flows, incident management and gather critical data about driving conditions.

But just as with any ICT system, this data and the on-board communication networks must be kept safe and secure. Data privacy extends to personal data captured by your car - think what someone could discover about your driving skills and habits! Similarly, hackers could create havoc, and potential tragedy, if they gained control of a car's electronic systems.

The 'E-safety vehicle intrusion-protected applications' (EVITA) project was one of the earliest EU-funded research activities to really concentrate on the issue of in-vehicle-network security. 'We focused on the security of the communication networks within the car,' explains Mr Henniger, the project's coordinator, 'but we were always thinking about parallel C2I and C2C networks under development. EVITA's on-board network security would be a cornerstone for all the other vehicle-

networking projects out there.'

Hard-wired security

There were many options for the EVITA partners to choose from. But after extensive evaluative studies and analysis of the security requirements, the team decided that the vehicle networks needed hard-wired cryptography. In other words, the scrambling and decoding of data would take place within a physical microchip - called a 'hardware security module' (HSM) - rather than via software.

One of the main benefits of using an HSM is its speed - it can encrypt data packets almost instantaneously, whereas software often involves a slight lag phase. Any processing delay cannot be tolerated in a vehicle travelling at over 100 kilometres per hour (kmph) - where even a 10th of a second interval could be the difference between life and death.

The EVITA team agreed on the specifications for the HSM, after looking at all the technology and protocols available and listening to the demands of the automobile industry. 'We investigated all the requirements and carried out a thorough risk analysis for all types of data transfer and connectivity within a vehicle. We specified the HSM to incorporate counter measures to reduce these risks,' says Mr Henniger.

'We realised that the automobile sector is very price sensitive, so we had to design our HSM with costs in mind,' Mr Henniger continues. 'We made sure that we did not over-specify the security requirements. We identified three levels of security: EVITA Lite, Medium and Full. The Lite version is used to transfer data from a small sensor to a central processing unit; this involves fairly innocuous data which people are unlikely to access and it does not need 'belt and braces' protection. At the other extreme EVITA Full offers the asymmetric cryptography, which is used whenever the car connects to outside networks to ensure the

integrity and authenticity of messages.'

Industry implementation

At present, while C2C and C2I remain in the laboratory, cars still do not typically incorporate data security features. But EVITA has paved the way to help make sure that the information will stay secure once cars get connected.

The EVITA HSM was designed through the combined research and expertise of the car manufacturer BMW Group Research and Technology, automotive suppliers such as Bosch and Continental, security experts including Fraunhofer SIT and EURECOM, software experts such as Fujitsu, and the hardware experts, Escrypt and Infineon.

The EVITA HSM has already proved its worth during C2C tests within the large-scale European 'Preparing secure vehicle-to-X communication systems' (Preserve) project. The vehicles under test originally deployed software-based asymmetric cryptography, but this proved slow and problematic. Replacing the software with the HSM led to a dramatic rise in speed and performance.

Cheaper chips

Since the EVITA project finished, the Preserve project has adapted the HSM design to alternative microchip manufacturing techniques. It is now possible to incorporate the HSM into smaller, cheaper ASIC chips.

'Based on the EVITA specifications, security can be added at minimal cost to data transfers and communication within the car, and as it connects to the outside world,' Mr Henniger concludes. 'By integrating this security via a chip we have made it much less prone to attack and

network hacking. As cars get clever and start to converse, I think drivers can rest easy. No-one is going to get hold of their data or suddenly start to take control of their car.'

More information: 'E-safety vehicle intrusion protected applications' project website
'Preparing secure vehicle-to-X communication systems', Preserve, project website

Provided by CORDIS