Secure updates for navigation systems and company

October 5 2011

At the push of a button by the driver, control units download the car manufacturer's new software -- such as enhanced map material for the navigation system. To ensure that this data channel is protected from hacker attack, the system needs the right cryptographic key. To date, these keys have been stored in each one of a vehicle's electronic control units.

Thanks to a new form of trust anchor, this will be simpler and more economical in the future. Researchers will present this process at it-sa, the IT security trade fair held October 11-13 in Nuremberg.

Imagine you live in Germany and want to take a few days of vacation in the French Alps. You have booked a hotel. To find it without having to thumb through road maps in hard copy, the navigation system must be retrofitted with French maps. To accomplish this, you either have to take a trip to the garage before setting out on the long journey, or you must obtain a CD with the appropriate data. The navigation system of the future however will download updates by itself at the driver's instruction. If the driver launches the program, the system returns numerous security questions – this is the only way to protect data transfer from hackers. Up until now, manufacturers have stored cryptographic keys on every device that is to download such manufacturer updates or communicate with other control units. If a device requests an update, first it must use the right key to prove that it is entitled to receive one.

This is just one example of an application in which cryptography plays a

decisive role in providing in-car protection. It is also the reason carmakers need to safely store numerous cryptographic keys in a vehicle's electronic control units. Researchers at the Fraunhofer Research Institution for Applied and Integrated Security AISEC in Garching near Munich have come up with a secure but economical method that accomplishes this. "We have developed a trust anchor – a device that securely stores cryptographic keys. Control units can use these keys, whether to request manufacturer updates or to communicate with one another," explains Alexander Kiening, a researcher at AISEC. But how does the process work? If a driver wants new map material for his or her navigation system, for instance, the system retrieves the key it needs from the central trust anchor. To do so, first it has to authenticate itself by demonstrating that the request really is coming from the navigation system; then it must prove that it has not been manipulated. To accomplish this, the trust anchor checks whether the software in the device matches the valid version. If this query is successful, the navigation system receives the key it can then use to establish a secure virtual private network data channel (VPN for short) to the manufacturer. It then downloads the desired software through this channel. Once this is complete, the updated device informs the trust anchor of a successful modification to the software.

The project is part of the group research project "Security in Embedded IP-based Systems (SEIS)" initiated by the German Federal Ministry of Education and Research (BMBF). Researchers have already developed a first demonstrator model in collaboration with Infineon, Continental and the Fraunhofer Research Institution for Communication Systems ESK.

Provided by Fraunhofer-Gesellschaft