A flexible solution for secure IT in cars

August 3 2015

The head unit demonstrator protects manufacturer data as well as vehicle users' private data by preventing unauthorized extraction. Credit: Fraunhofer SIT

Today, almost everything in your car is managed by an electronic control unit (ECU). The problem is that these minicomputers are increasingly coming under attack. Fraunhofer researchers have now developed a platform that makes it possible to flexibly install secure devices in a way

that is based on open and vendor-neutral hardware and software standards.

Cars are as much a part of the digital revolution as anything else – ECUs are used in controlling the engine, steering and braking. They can improve road safety, automatically call for help in emergencies and guide drivers to their next destination quickly and safely. Today's cars contain over 100 of these minicomputers. "IT has become one of the greatest drivers of automotive innovation," says Dr. Christoph Krauß of the Fraunhofer Institute for Secure Information Technology SIT in Darmstadt, Germany. His focus is on IT security in vehicles. "Cars used to be closed systems, but today's IT interfaces are making them increasingly vulnerable to attacks," Krauß adds. There is no shortage of current examples either – hackers mine personal information, used-car dealers tamper with odometers, car thieves open doors and cheat immobilizers, and car tuning enthusiasts enable functions they haven't paid for. As technology continues to advance, it's becoming increasingly important to improve IT security in vehicles. "There are of course cryptographic solutions out there, but these tend to lack the required flexibility," Krauß says.

Development platform based on new security standards

Krauß and his colleagues have built a solution that uses hardware security modules (HSMs) for device protection. It's based on the latest version of the Trusted Platform Module – TPM 2.0 – an international open standard developed by the Trusted Computing Group. Almost all major IT companies are members of this consortium and they have been working together for over ten years to establish standards. For its part, Fraunhofer SIT shares its expertise in hardware-based security solutions. "Our solution is a software platform for developing secure ECUs based

on TPM 2.0. It allows you to first simulate all essential vehicle ECU elements – hardware and software – for virtually any application before implementation," says project manager Andreas Fuchs. "This provides manufacturers with important information during development, which means they can reconstruct a range of application scenarios and iron out any kinks. They need to do this because they can't have a peek into real, completed HSMs for security reasons."

Depending on exactly what needs to be protected, TPM-based solutions developed using the new platform can either be installed directly into a given ECU or preset for it. The solution's hardware acts as a "trust anchor": A secure place for storing cryptographic keys and an execution environment for all security-relevant operations. It detects attacks and releases the key only when it is sure the device is working reliably. "Say someone has interfered with a car's parking assistance feature. In that case, the engine's ECU will prevent the car from starting. That means the parking assistant can't affect steering behavior in a way that may cause injury," Krauß says. The job of HSM software is to communicate with the hardware and to ensure that the security functions provided are embedded in the ECU's core tasks. Using this framework, the Fraunhofer SIT research team developed an HSM demonstrator for a head unit, which is used to control a car's infotainment features. This head unit protects both manufacturer data as well as vehicle users' private data by preventing unauthorized extraction.

"TPM security modules can now be found in almost every desktop and laptop computer; for example, they safeguard the BitLocker drive encryption program for Microsoft Windows," Fuchs says. "Our development environment is helping the TPM standard to become more widely used in automotive applications. It's now easier for manufacturers to implement security standards as well as the applications based on them. What's more, the platform could also be used in other sectors – for instance, as a secure means of controlling industrial plants or for

application in the Internet of Things." The technology is already in line to be licensed for two industrial applications and the researchers are very close to a finished automotive product. Krauß concludes, "It's clear that we're heading towards a world of automated driving, which only underlines the importance of automotive IT security."

Provided by Fraunhofer-Gesellschaft