Secure radio signal for central locking

February 1 2010

An asymmetric algorithm in this car key ensures high security when the car door is unlocked by radio signal, but does not drain the battery. (© Fraunhofer SIT)

(PhysOrg.com) -- Remote central locking is among the most convenient aspects of modern motoring. Transmission of the radio signal that activates the system is not particularly secure, however. A new encryption technique increases security without draining the key's battery.

Most drivers love the convenience of remote central locking - the car doors are locked or unlocked just by pressing a button on the key. These systems are not particularly secure, however, as a potential car thief can, for example, use an antenna to eavesdrop on the radio signal and create a second key from the captured data on a computer.

The reason for this weakness in security is that the algorithms which encrypt the signals sent from the key to the vehicle are not strong enough. Their code was broken about two years ago. Car manufacturers are therefore using new algorithms to make the radio key systems more secure. But these algorithms too have a major disadvantage - they are symmetric, their codes are embedded in the key and in the car. Also, the same coded information is embedded in numerous vehicles from the same production line. Once one code has been broken, numerous cars are at risk.

Research scientists at the Fraunhofer Institute for Secure Information Technology SIT in Garching, Germany, have now used an asymmetric algorithm to develop a car key prototype for the first time. "With this type of algorithm the secret is only located in the car key, and not in the car as well," explains Johann Heyszl, a scientist at the SIT. "Each car key incorporates a different code, and this makes the encryption much more secure than when a symmetric algorithm is used."

Up to now the high computation intensity and associated high energy consumption posed a high barrier against the use of asymmetric algorithms. "We have built a small cryptographic chip which is particularly energy-saving. In addition, we have developed a new, efficient protocol which minimizes computation effort and the amount of data that has to be transmitted," says Heyszl. As a result, the battery life of the key is about the same as in symmetric encryption, but the new system is much more secure. The electronic immobilizer is encrypted in the same way as remote central locking.

The research scientists have already developed a functioning prototype and will be presenting the system at the Embedded World trade show from March 2 to 4 in Nuremberg, Germany.

Provided by Fraunhofer-Gesellschaft