New security technology for the 'Internet of Things'

18 June 2015

Washing machine, smoke detector, burglar alarm and refrigerator - all of those and many appliances more could in future be connected to the Internet. To ensure that the connected home does not turn into a security hazard, IT researchers at the Horst Görtz Institute at the Ruhr-Universität Bochum (RUB) have developed new protection technologies for the "Internet of Things", which they are now getting ready for the market. The Federal Ministry for Economic Affairs and Energy backs the start-up idea "PHYSEC" with approx. 650,000 euros under the umbrella of the programme "EXIST research transfer".

Fast, resource-efficient and secure

In the future, many household appliances will be gathering data in their home environment and communicate them through wireless connections. "This is why data security is of crucial importance," says project manager Christian Zenger. "Because wireless communication doesn't stop at the front door." Using a combination of digital encryption and analogue communication technologies, the start-up team from Bochum wants to enable security in the wireless communication between small devices. The technology is fast, energy-efficient and facilitates high security levels. A demonstration system that works effectively is already available.

Technology based on random number generator

The technology is based on a random number generator. It grants two parties that conduct wireless communication access to a synchronised sequence of random numbers. From this sequence cryptographic keys can be derived, for example. These keys are only shared by pairs of communication partners and not by all devices within the network. Thus, the problem associated with a single key shared by all devices has been solved: "Attacks may scale strongly, that means, for example, that an entire factory could become completely hackable once one small sensor had been stolen and analysed," explains Zenger. This danger does not arise with the "PHYSEC" system. Moreover, the key changes regularly; thus, many advanced attacks become less effective and, ideally, inapplicable.

Integrating new appliances via mobile phone into the secured network

A mobile phone app will be available to include new devices into an already existing "Net of Things" secured by "PHYSEC". "All the user has to do is hold his Smartphone a few centimetres in front of a new device," says the researcher from Bochum. The app enables the authentic exchange of a unique cryptographic key that is exclusively assigned to the new device. "This is how future cyber-physical systems are connected to the network in a secure and user-friendly manner," says Zenger. "The entire process is very intuitive and does not have to be handled by an IT expert." The "PHYSEC" team plans to file a patent application for its technology.

The people involved in "PHYSEC" are Christian Zenger, PhD student at the Chair for Embedded Security, Dr Benedikt Driessen, who completed his PhD degree at RUB in 2013 and is currently on the payroll of "Infineon AG", Heiko Koepke, PhD student at the Chair for Controlling, and RUB student Jan-Felix Posielek.

Provided by Ruhr-Universitaet-Bochum