Researchers discover security flaws in smart home products

5 September 2017

Credit: Philipp Morgner

Smart home products such as lamps controlled via mobile devices are becoming ever more popular in private households. We would, however, feel vulnerable in our own four walls if strangers suddenly started switching the lights in our homes on and off. Researchers at the IT Security Infrastructures group, Friedrich-Alexander University Erlangen-Nürnberg (FAU) have discovered security problems of this nature in smart lights manufactured by GE, IKEA, Philips and Osram.

Philipp Morgner and Zinaida Benenson's team managed to make connected lighting systems of different manufacturers flash for several hours with a single radio command sent from a distance of more than 100 metres away. Additionally, they were able to modify the bulbs using radio commands so that the user was unable to control them. It was even possible in certain situations change the colour or brightness of the light.

Inadequate security features

The FAU researchers discovered the security weaknesses in ZigBee, an important wireless standard employed for the control of smart home products. More than 100 million products that use ZigBee technology are estimated to have been distributed around the world. The most recent version, ZigBee 3.0, was released in December 2016. Part of this specification includes the touchlink commissioning procedure for adding new devices to an existing smart home network or to set up a new network. The team was able to demonstrate that the security features of touchlink commissioning are inadequate and make it vulnerable to attack. It is probable that other applications based on ZigBee that are relevant to security, such as heating systems, door locks and alarm systems, will also be affected in the future.

Manufacturers react to security risk

The research team recommended disabling touchlink commissioning in all future ZigBee 3.0 products. Some manufacturers have already reacted and made an update available to customers that significantly reduces the risk of an attack. The latest information is published on the a website.

The IT Security Infrastructures group focuses on IT security in the context of the Internet of Things. The researcher's findings show that most manufacturers consider security issues to be less important than functionality and compatibility requirements. That is why the team has decided to identify vulnerabilities to motivate manufacturers to develop better security measures.

Provided by University of Erlangen-Nuremberg