More rules for the intelligent household

October 24 2018

The results show which user groups should be able to control which capabilities of smart home devices according to the study participants. The researchers did not ask whether children should be able to control mowers and lights, since these functions can currently only be controlled via the smartphone and the researchers assume that eight-year-old children generally do not have their own smartphone. Credit: Agentur der RUB, Maximilian Golla

While a mobile phone or PC is traditionally controlled by only one user, many players come together in a networked household, some of whom even want to control devices simultaneously. Researchers from the Horst Görtz Institute for IT Security at Ruhr-Universität Bochum, together with colleagues from the University of Chicago and the University of Washington, have investigated what access control for internet-

connected household appliances should ideally be like. They interviewed 425 users in the USA about their preferences and derived suggestions for access management from these.

The team presented the results at the Usenix Security Symposium in the USA in August 2018. The science magazine Rubin at Ruhr-Universität reports in detail about the study.

The researchers first analysed which smart home devices are currently on the market, what capabilities they possess, and how access rights to them can be managed. "In rare cases, there is a guest group with other access rights in addition to the administrator or owner, who is allowed to do everything," says Maximilian Golla, doctoral candidate in the Bochum-based Mobile Security Research Group headed by Professor Markus Dürmuth. However, much more complex social relationships occur in a household.

The scientists based their online survey on six potential user groups: spouses, eight-year-old children, 16-year-old teenagers, visiting family members, babysitters, and neighbours. They also selected 22 capabilities that smart home devices can have, such as playing music, shopping online, turning lights on or controlling door locks. For each capability, they asked the participants whether the respective user group should have access to it. The respondents were able to answer: always, sometimes, or never.

When a respondent answered "sometimes", they had to specify how it would be determined whether or not the person should be able to use the function. From these responses, researchers derived a number of contextual factors that affect access rights, such as age, where the person or device is located, whether the person has used the device before, the time of day, and the cost of using it.

Using all the data from the survey, the IT researchers created a profile of the capabilities that each user group should be able to use by default. According to the study participants, for example, the spouse should have almost all rights, the neighbour almost none. For the other user groups – teenagers, children, visiting family members, and babysitters – there were four different combinations of desired and undesired capabilities.

However, it is also important that the system is not so complicated that the users of internet-connected households no longer want to deal with the plethora of access restrictions. "The data collected can be used to derive standard settings for the six selected roles, which the user would then only have to adjust if necessary," explains Golla.

In the future, the researchers want to investigate how access restrictions for smart home devices could be managed in a user-friendly way using a rule language.

More information: Rethinking access control and authentication for the home Internet of Things (IoT), Usenix Security Symposium, Baltimore, USA, 2018, www.usenix.org/conference/usen … ty18/presentation/he

Provided by Ruhr-Universitaet-Bochum