Tobias Giertz

Theme: Smart Home

Smart homes, an aspect of the Internet of Things, offer the promise of improved energy efficiency and control over home security. Integrating various devices together can offer users easy programming of many devices around the home, including appliances, cameras and alarm sensors. Several systems can handle this type of task, such as Google Brillo/Weave, Apple HomeKit or Amazon Alexa.

But there are also security risks. Smart home systems can leave owners vulnerable to serious threats, such as arson, blackmail, theft and extortion. Current security research has focused on individual devices, and how they communicate with each other. For example, the MyQ garage system can be turned into a surveillance tool, alerting would-be thieves when a garage door opened and then closed, and allowing them to remotely open it again after the residents had left. The popular ZigBee communication protocol can allow attackers to join the secure home network.

Little research has focused on what happens when these devices are integrated into a coordinated system. We set out to determine exactly what these risks might be, in the hope of showing platform designers areas in which they should improve their software to better protect users' security in future smart home systems.

My statements were additionally supported by the following sources:

https://tech.co/smart-homes-security-risks-2016-05

Excerpts from the Guardian news article (teaching materials)