Smart Health describes electronic-based diagnosis and treatment systems (e.g., blood pressure monitors, scales, thermometers), special sensors (e.g., fall sensors, sensors in the toilet, heat sensors), wearables (e.g., smart watches, fitness trackers or smartphones) up to intelligent body modifications (e.g., implants or prostheses) which are connected to each other. By networking these and combining several such items, new functions and services become possible that offer added value over the individual item. The diagnostic/treatment/sensor devices can often be connected to another device, e.g., wearables or smartphones, and thus additionally controlled.

This new technology brings a number of improvements:

- Improved information for doctors, e.g., blood pressure measuring instruments reporting and transmitting regular measurements
- Improved health, e.g., fitness trackers analyzing your sleep patterns
- Improved emergency response, e.g., fall detectors sending a direct emergency message to the rescue service

Many users assume that their devices are already by default set by the manufacturer to protect their privacy or security. However, not every manufacturer has an interest in the devices being set up for maximum privacy protection. On the one hand, some manufacturers are interested in the additional data. On the other hand, maximum privacy or security sometimes goes hand in hand with a loss of functionality. Since you don’t know beforehand what the manufacturer’s attitude towards privacy and security is, you should look at the settings during configuration. This is the only way to ensure that your own preferences are guaranteed.

Therefore, it is important that you take sufficient time to configure your smart health devices in terms of security and privacy. In addition, while using the smart health devices, you should carefully read any messages that may occur and act according to the instructions.

Contact

Karlsruhe Institute of Technology (KIT)

Institute for Applied Informatics and
Formal Description Methods (AIFB)

Research Group Security • Usability • Society (SECUSO)

Prof. Dr. Melanie Volkamer
Kaiserstraße 89, Bldg. 05.20
76133 Karlsruhe, Germany

Phone: +49 721 608 450 45
Email: kontakt@secuso.org

secuso.aifb.kit.edu
twitter.com/secusoresearch

Issued by

Karlsruhe Institute of Technology (KIT)

President Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe, Germany
www.kit.edu

The content of the leaflet is based on the European Unions Horizon 2020 research and innovation programme under grant agreement No 740923, project GHOST (Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control).

KIT
Karlsruhe Institute of Technology

aifb

Smart Health Risk

Learn more about security
and privacy risks

INSTITUTE OF APPLIED INFORMATICS AND
FORMAL DESCRIPTION METHODS (AIFB)

SECUSO
SECURITY · USABILITY · SOCIETY

KASTEL

In this leaflet you will find more information about security and privacy risks and their consequences.

Security Risk

Hackers can harm you in many ways: If hackers gained access to your smart home devices, data and information stored in or generated with the devices can be spied out. Furthermore, hackers can then control your smart home devices and also reconfigure them, e.g.,

- take control of sensors (this allows them, e.g., to capture sensitive data such as blood pressure or pulse),
- change room temperatures considerably (e.g., your plants or animals in the house suffer as a result),
- manipulate sensor data (this results, e.g., in fall sensor mistakenly sending emergency calls),
- manipulate wearables (this results, e.g., in spontaneous loud sounds for no reason),
- overload toilet sensors (this results, e.g., in the toilet being destroyed or your electricity bill being increased),
- manipulate connected implants or prostheses (this results, e.g., in the durability decreasing or the body modifications being destroyed),
- take control of remote maintenance of the devices (e.g., this allows devices in the house to be switched on/off and leads to life-threatening situations).

Privacy Risk

The manufacturers of smart health devices collect a variety of data and information, e.g., credit card information while shopping, information about your online purchases, current room temperature, search queries made so far, light activity, weight or information about movements within the home of those present. Sometimes data is collected which is only possible through additional functionality that has been activated with subsequent updates. Consent to this additional data collection is then sometimes deeply hidden in the new agreements and is not always clearly recognisable.

Your usage habits are derived from this data (e.g., on which days you switch on light and heating and at which times, at which times and on which days you prepare your coffee, do your laundry or which food you buy online, your preferences for TV and Internet shows). This allows manufacturers to create extensive usage profiles of you. These are used by the manufacturers of your devices or the app manufacturers on your devices, among other things, to improve their services or for remote maintenance of the devices/services.

However, if the data collected and the usage profiles created fall into the hands of third parties or are used by the manufacturer for other purposes contrary to the agreement, you may suffer damage in a variety of ways.

Third parties can access this data, information or usage profiles either because

- you have explicitly (possibly unconsciously) allowed the manufacturer of the Smart Health devices or apps to do so.
- criminal employees of the manufacturer want to enrich themselves financially and therefore illegally copy the data and pass them on or sell them to third parties.
- hackers exploit security gaps in the systems and/or servers of the manufacturers and thus gain access to the data, information or usage profiles. Then hackers can either publish them or blackmail you by threatening to publish them, sell them to third parties or use them themselves to harm you.

Examples for concrete consequences

- The Information from the combination of different profiles (e.g., lighting activity, temperature control and power consumption) can be used to carry out targeted burglaries.
- Your health data may, if passed on to your current or potential employer, result in you having a less chance of applying for a new job or being fired.
- Your personal preferences may be used, if passed on or sold to other companies, to influence your purchase decision or to make products that you are likely to buy more expensive.
- Your health data (e.g., blood pressure, clinical record, medicines), if passed on to your bank, can lead to worse conditions for a loan.
- Your location data may cause you to become a victim of stalking.
- Your data about your living conditions (e.g., from mapping of your apartment), can be used to make conclusions on your financial situation and thus lead, e.g., to more expensive interest in the mail order business.
- Your preferences, your devices and your communication data may be used, if passed on to third parties, to influence your decisions, e.g., in political elections.
- The combination of dietary respectively sports preferences and blood pressure can be used, if passed on to your insurance company, to limit you in your way of life if you do not want to be put into a more expensive insurance premium.
- Your personal information (name, address, gender or bank details) may be used to take over your digital identity and publish inappropriate content, send dangerous messages (e.g., phishing messages or messages with dangerous attachments) or carry out financial transactions on your behalf. Conflicts with friends can also arise when confidential content is published.
- Your fitness, health or sensor data may result in you not feeling undisturbed at home anymore. Therefore, you might restrict yourself in your behavior or feel restricted.

All these are examples that have already appeared in practice. The dangerous thing about collecting and evaluating data and information about your own usage habits is that it is not yet possible to predict what can be derived from the data in the future, e.g., which diseases a person has or the truthfulness of statements you make to other people.