Technische Universität München, Department of Informatics

Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

Thesis M.Sc.

Decentralized, privacy-preserving processing of sensor data

Motivation

Smart buildings are equipped with several kinds of sensors like temperature, motion, and power consumption. All those sensors can be used to derive higher level information like the presence of persons in a given room. Given more technological equipment like transponders for authentication in the same environment those sensor information can even become person-related. I.e. Alice opening the door to the meeting room allows sensors to exactly determine the length of her presence and might even enable sensors on the corridor to track her after she left it again.
Hence, privacy of persons in a smart building is a hot topic in academia and industry right now. Partially it also gains relevance as the processing of personal data requires data protection laws to be applied when a smart building shall be installed. In consequence, a desirable improvement is to reduce the amount of personal data to a minimum and also reduce the amount of system components which actually have to cope with them as that reduces the necessary legal effort.

Approach

We have a decentralized software architecture in mind that consists of several trusted but local room controllers. Each controller is responsible for its dedicated area in the building (e.g., a room). A controller will primarily deal with local sensor information and influence the local area only (e.g., turn off the heating in its room). The major benefit of this locality principle is that no critical data leaves the controller without the users consent which mitigates the privacy issue.
However, use cases exist, where controllers of other building parts also need sensor data from local areas (e.g., the presence of any persons in a building section). For such cases the room controller shall provide means for secure data exchange. One can also think of privacy-enhancing techniques which remove or at least decrease the level of person-relatedness of the data transferred.

Your Task

Given an example scenario regarding energy consumption, you develop an architecture which is based on VMs. You have to make them secure (think of dm-crypt, GPG, etc.) so that they become a personal trustworthy device. Then, they must be able to cope with the data, provide secure transfer of information between VMs and keep track with whom it already shared which data.

Requirements

Python or Java, Linux, basic network security knowledge, self-dependence.

Contact

Dr. Holger Kinkelin kinkelin@net.in.tum.de
Marcel von Maltitz vonmaltitz@net.in.tum.de