Requirements and Mechanisms for Smart Home Updates

Peter Zdankin
University of Duisburg-Essen
Duisburg, Germany
peter.zdankin@uni-due.de

Marian Waltereit
University of Duisburg-Essen
Duisburg, Germany
marian.waltereit@uni-due.de

Viktor Matkovic
University of Duisburg-Essen
Duisburg, Germany
viktor.matkovic@uni-due.de

Torben Weis
University of Duisburg-Essen
Duisburg, Germany
torben.weis@uni-due.de

***Abstract*—Devices forming a smart home should be updated regularly over their life-time. Often enough this update process introduces new problems or errors in the system. For this reason, we will define requirements for an improved smart home update process. The goal is to detect faults and incompatibilities early in the process and thus to give users advice in what to update and when. Thus, each smart home installation needs to find its optimal update configuration. Updates are created by various vendors and may not only add but also remove functionality on individual devices. Furthermore, some device manufacturers are more eager to update than others. Thus, missing updates for some devices mean that available updates for others should not be installed, because of resulting incompatibilities. This is essentially true for security updates that affect the protocols used. When users decide to update their smart home, there are bad update configurations, in which essential functionality breaks and good configurations, which enable new useful services and improve security. To find ideal update configurations, we first need to define what optimality means in this context, because different configurations will result in different feature sets or security levels. Furthermore, each user might have different preferences resulting in different optimal configurations for each user and system. In an ideal case, every smart home installation can figure out optimal configurations locally, because of privacy and security concerns of sharing smart home configurations and potential security issues with external entities. That means, in the ideal case there is no dependency on external services and each installation works autonomously. However, in this setting self-description of smart home devices becomes essential to enable local decision making. Unfortunately, self-description is not always perfect, because it is either lacking, outdated, or does not exactly describe the actual implementation. Therefore, other options involving external services need to be considered as an alternative. Such an external (and commercial) service could thoroughly test devices and software versions to verify that they comply to specified protocols and self-descriptions. Furthermore, the external service could gather usage data from many smart home installations and draw conclusions from real-world usage data. However, this means that data about installed smart home systems and their usage is sent to an external service, which raises privacy questions and means that the smart home is no longer autonomous. In this paper we compare approaches with and without external services, as each may have benefits that may outweigh the drawbacks. Thus, we evaluate the different approaches against our requirements to show the trade-off between optimality of configurations on one hand and privacy autonomy on the other hand.**