

Ibrahim Armaç: Personalized eHomes: Mobility, Privacy, and Security

Promotion: RWTH Aachen, Fakultät für Mathematik, Informatik und Naturwissenschaften

Erstgutachter: Prof. Dr.-Ing. Manfred Nagl, RWTH Aachen

Zweitgutachter: Prof. Dr. Dr. h.c. Otto Spaniol, RWTH Aachen

Datum der Prüfung: July 06, 2010

Veröffentlichung: Shaker-Verlag, AIB-SE 5, 316pp, 2010

Kurzfassung:

eHomes are intelligent environments providing value-added services to their users. These services realize complex functionalities by combining basic functionalities of various devices and appliances. Reasonable eHome services can be identified in the domains of comfort, security, multimedia, energy consumption and eHealth.

There exist several challenges which need to be addressed when developing and operating eHomes. First, the heterogeneity of various device types and standards must be overcome in order to ensure the interoperability of eHome services. Second, changes which result from various kinds of dynamics must be taken into account at runtime. Third, adequate concepts are required for personalizing eHome services so that their functionalities can be adapted to individual user preferences. Finally, multilateral security must be provided to users and eHomes.

Several tools have been developed in previous dissertations at the Software Engineering group for addressing the heterogeneity problem. These tools enable the reuse of component-based eHome services by a specification, configuration, and deployment process (SCD Process). Moreover, the structure of a service composition, resulting from the SCD Process, can be adapted while the system is running. Thus, an eHome can handle the abovementioned dynamics.

In this thesis, I have worked on two essential aspects of eHomes which have not been considered in previous dissertations.

First, I have investigated how users can be supported in personalizing eHomes in the context of inter-eHome mobility, a special kind of dynamics. This term describes the situation where users often move from one eHome to another one. The aim is to adapt eHome services to the preferences of the mobile users possibly without an additional configuration overhead. For this purpose, I have extended the existing eHome prototype. It now enables two kinds of eHomes personalization. First, I have developed a mobile user model which can be used to store and manage user preferences on a mobile device and provide them to visited eHomes when necessary. As a result, redundant management effort is avoided. Second, mobile users now can take along and execute per-

sonal services on their mobile devices. These services can remotely interact with basic services which are executed in the visited eHomes and control the devices required for realizing their functionalities. Hence, the users can benefit from habitual functionalities even in such eHomes which do not offer these functionalities by their own services.

Second, I have worked on the realization of multilateral security in the context of inter-eHome mobility. In doing this, I considered the security objectives of both the users and the eHomes.

For protecting the user privacy, I have developed concepts based on the principles of data minimization and unlinkability of user data. For minimizing the data disclosed to eHomes, I have introduced a negotiation-based identity management system. Furthermore, this system enables mobile users to interact with each eHome by another identity. In addition to that, an authentication mechanism based on anonymous credentials avoids the linkability of user data by colluding eHomes.

For protecting eHome services against unauthorized access by both users and services, I have realized a combination of credential- and role-based access control mechanisms. On the one hand, they fulfill accountability requirements. On the other hand, the roles can be automatically adapted to evolving service compositions at runtime of an eHome.

The described concepts have been realized in form of new tools. The applicability and the evaluation of the achieved results have been shown in different test scenarios. For this purpose, I have developed different software demonstrators simulating eHomes.

Concluding, this thesis accommodates personalization to privacy protection, two reluctant requirements, by providing a sound compromise between anonymity and accountability. Due to this, mobile users can benefit from personal services in different eHomes while their privacy is protected. As a result, this work contributes to the acceptance of eHomes in a future mass market.