Future Generation Computer Systems 56 (2016) 719–733

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A risk analysis of a smart home automation system

Andreas Jacobsson[a,*], Martin Boldt[b], Bengt Carlsson[b]

[a] *Department of Computer Science, Malmö University, 205 05 Malmö, Sweden*

[b] *Department of Computer Science and Engineering, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden*

HIGHLIGHTS

- Smart home automation systems introduce security and user privacy risks.
- A risk analysis of a smart home automation system is designed and conducted.
- 32 risks are identified, of which four are classified as severe and 19 as moderate.
- The severe risks are related to the software components, as well as human behavior.
- It is concluded that security and privacy should be integrated in the design phase.

ARTICLE INFO

Article history:
Received 13 November 2014
Received in revised form
11 June 2015
Accepted 4 September 2015
Available online 14 September 2015

Keywords:
Internet of Things
Smart home automation
Risk analys
Privacy
Security

ABSTRACT

Enforcing security in Internet of Things environments has been identified as one of the top barriers for realizing the vision of smart, energy-efficient homes and buildings. In this context, understanding the risks related to the use and potential misuse of information about homes, partners, and end-users, as well as, forming methods for integrating security-enhancing measures in the design is not straightforward and thus requires substantial investigation. A risk analysis applied on a smart home automation system developed in a research project involving leading industrial actors has been conducted. Out of 32 examined risks, 9 were classified as low and 4 as high, i.e., most of the identified risks were deemed as moderate. The risks classified as high were either related to the human factor or to the software components of the system. The results indicate that with the implementation of standard security features, new, as well as, current risks can be minimized to acceptable levels albeit that the most serious risks, i.e., those derived from the human factor, need more careful consideration, as they are inherently complex to handle. A discussion of the implications of the risk analysis results points to the need for a more general model of security and privacy included in the design phase of smart homes. With such a model of security and privacy in design in place, it will contribute to enforcing system security and enhancing user privacy in smart homes, and thus helping to further realize the potential in such IoT environments.

1. Introduction

In the near future, it is estimated that somewhat 90 million people around the world will live in smart homes, using technology to improve home security, comfort, and energy usage [1]. A recent study has shown that more than every fourth person in Sweden feels that they have poor knowledge and control over their energy use, and that four out of ten would like to be more aware and to have better control over their energy consumption [2]. A solution is to provide the householders with feedback on their energy consumption, for instance, through a smart home automation system [3]. Studies have shown that householders can reduce energy consumption with up to 20% when gaining such feedback [2,3]. Smart home automation is a prime example of a smart environment built on various types of cyber–physical systems generating volumes of diverse, heterogeneous, complex, and distributed data from a multitude of applications and sensors. Thereby, such home automation is also an example of an Internet of Things (IoT) scenario, where a communication network extends the present Internet by including everyday items and sensors, which in this case includes the possibility to monitor and manage energy usage [4]. As such, smart home automation systems incorporate common devices that control features of the home, but they do not only turn devices on and off [5]. For instance, smart home automation systems can monitor the configuration of the internal environment and the activities that are being undertaken whilst the house is

[*] Corresponding author. Tel.: +46 709 655 209; fax: +46 40 665 76 46.
E-mail address: andreas.jacobsson@mah.se (A. Jacobsson).

http://dx.doi.org/10.1016/j.future.2015.09.003
0167-739X/© 2015 Elsevier B.V. All rights reserved.

occupied (and unoccupied). The result of these modifications to the technology is that a smart home automation system can autonomously operate devices and thus manage the home on behalf of the end-users, i.e., humans.

Smart home automation is attracting more and more attention from commercial actors, such as, energy suppliers, infrastructure providers, and third party software and hardware vendors [6,3]. Among the non-commercial stakeholders, there are various governmental institutions and municipalities, as well as, end-users. Knowledge, tools, and infrastructures related to software and data have begun to evolve in order to cover the challenges brought on by the complexity and the heterogeneity of massively interconnected services and devices, but there is at this point no well-established practice to design such intelligent systems [7]. For instance, accepted reference architecture alternatives or software platforms, let alone such that include otherwise crucial system requirements, such as, security and privacy in the process are currently missing [7,8]. As a result, there are multiple vertical solutions where vendors claim to support the whole chain from the sensors and devices to the gateways and servers, with whatever dedicated software that is appropriate in the perspective of the specific company. For example, this includes highly specialized APIs for the integration of additional services on top of the existing solutions. This creates a complex situation where, among many things, it is hard to avoid customer lock-in, something which may further smother their involvement and commitment. As a consequence, this also creates difficulties for executing system-hygienic tasks, such as, analyzing risks, enhancing privacy, and enforcing security in these environments.

In a joint research project involving leading industrial actors in the segment of home/building automation, a common interface of a smart home automation system (hereinafter denoted SHAS) that combines various vendors' systems has been developed.[1] Using SHAS, it is possible to transparently manage several smart home automation systems simultaneously in real-time. It is also possible for third party stakeholders, such as, property owners and municipalities, to both monitor energy consumption and remotely control electronic devices in the homes and buildings. Furthermore, end-users (e.g., as tenants) can collect aggregated energy consumption statistics on their buildings (e.g., from the owners). Based on the collected data, various services can be implemented, primarily as a way to raise the energy-awareness among end-users, e.g., by using gamification approaches. Also, on top of the common interface, an open mobile platform for energy efficiency services allows end-users to access various applications through an ecosystem of online services and smartphone applications. Through an open API, it is also possible for third party developers to connect their services and applications. In the research project, SHAS is tested on an apartment complex situated in Malmö, Sweden.

In IoT systems, particularly in those that involve human actors, such as, our SHAS, understanding the risks related to the use and potential misuse of information about customers, partners, and end-users, as well as, forming methods for integrating security-enhancing measures in the design is not straightforward and thus requires substantial analysis [4,9]. In addition, measures ensuring the IoT architecture's resilience to attacks, such as, authentication, access control, and user privacy need to be established [10]. In fact, the difficulty in achieving security in IoT environments has been identified as one of the top barriers of smart home automation [7], underlining that this is a cumbersome, yet important task.

In this paper, we apply a common risk analysis method in order to evaluate system vulnerabilities and threats, as well as, their likeliness of occurrence and potential impacts, i.e., the system's risk exposure. The analysis of risk exposure in SHAS is thus based on the well-known Information Security Risk Analysis (ISRA) method, documented by, e.g., Peltier [11]. The application of ISRA on SHAS is founded on a review of current advancements in science and industry. In order to fully understand the scope of the consequences brought on by smart homes, it is crucial to analyze not only the system risks related to privacy and security, but also the types of scenarios with respect to user privacy and home security that they entail. The main contribution is thus the results of the risk analysis on the smart home automation system in combination with the scenarios highlighting the consequences to user privacy and the review of the state of the art.

The paper is organized as follows. First, we set the scene by introducing the potential risk scenarios with respect to security and privacy of smart home automation. Then, related work, the architecture of SHAS, the ISRA method and its results are accounted for. This is followed by a discussion about the general risk exposure in relation to the main observations from the literature and scenario descriptions. In the end, conclusions and pointers for future work are summarized.

2. Scenarios of the private/public home

Before examining the risk exposure of SHAS by applying ISRA, we pinpoint some common scenarios for smart home automation systems. These scenarios have emerged as a result of discussions with key stakeholders within the smart home automation industry, i.e., the industry partners of the project management group of SHAS.

Property, as well as, users and the information that they are generating constitute an integral part of smart home automation, and as smart home automation systems become increasingly more adopted by residents, these system-infrastructures are also gaining more interest from other industry sectors. This is much due to that smart home automation systems introduce a valuable platform for direct user involvement, often through various connected sensors within the home environment where users and property interact through tablets, smartphones, computers, and various wearable devices. Future possibilities to extend the benefits and services of smart home automation will emerge that bring about a risk of concept drift. Basically, new vendors benefit from the context-aware smart home infrastructure, for instance, by exploiting the possibility of adding novel products and services to the ecosystem. Vendors take part in ecosystems, with business connections to various other vendors, rendering in that security and privacy concerns are often neglected or ignored. Another side of this is that the system (in our case SHAS) is reconfigured and equipped with new devices and software not included nor taken into account in the original design, rendering in that the system must be considered to be neither stable nor static; it is dynamic and changes all the time, and also in ways that are difficult to predict.

To shed some light on scenarios entailed by this development, we will now discuss the incorporation of safety surveillance cameras within a smart home, digital traces, and the addition of connected devices in smart homes. Below, these scenarios are briefly introduced and are then revisited in 7.

2.1. From energy efficiency to safety surveillance cameras

Even though smart home automation systems, such as SHAS, may be originally intended for energy efficiency support, it can be extended to include also other types of appliances in the homes. In smart homes, the use of a safety surveillance camera typically has a purpose to detect anomalies in the home environments, i.e., events that differ from the daily use. A first example of such an anomaly is

[1] More information can be found at http://elis.mah.se/ Last accessed: 2015-06-02.