On the Risk Exposure of Smart Home Automation Systems

Andreas Jacobsson
Department of Computer Science
Malmö University
205 06 Malmö, Sweden
andreas.jacobsson@mah.se

Martin Boldt and Bengt Carlsson
Department of Computer Science and Engineering
Blekinge Institute of Technology
371 79 Karlskrona, Sweden
{martin.boldt;bengt.carlsson}bth.se

Abstract— **Achieving 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 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 investigation. A risk analysis applied on a smart home automation system developed in a research project involving leading industrial actors has been conducted. 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 in nature.**

Keywords—Internet of Things, smart home automation, risk analys, privacy.

I. Introduction

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 consumption [5]. A solution is to provide the householders with feedback on their energy consumption, for instance, through a smart home automation system [10]. Studies have shown that householders can reduce energy consumption with up to 20% when gaining such feedback [5][10]. 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, 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 [22]. Home automation is attracting more and more attention from commercial actors, such as, energy suppliers, infrastructure providers, and third party software and hardware vendors [8][10]. Among the non-commercial stakeholders, there are various governmental institutions, 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 inter-connected services and devices, but there is at this point no well-established practice to design such intelligent systems [4]. 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 [4][17]. 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 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 (SHAS) that combines various vendors' systems has been developed[1]. Using the common 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 are being 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 API, it is also possible for third party developers to connect their services and applications. In the research project, the common SHAS is tested on an apartment complex situated in Malmö, Sweden.

In highly connected ecosystems, 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 [22][24]. In addition, measures ensuring the IoT architecture's resilience to attacks, authentication, access control, and user privacy need

[1] More information can be found here: http://elis.mah.se/

to be established [25]. In fact, the difficulty in achieving security in IoT environments has been identified as one of the top barriers of smart home automation [4].

In this paper, we outline a method for reviewing probable dangers, i.e., system vulnerabilities and threats, as well as, their likeliness of occurrence and potential impacts, i.e., the system's risk exposure. The risk analysis is based on the well-known Information Security Risk Analysis (ISRA) method, documented by, e.g., Peltier [21]. In this qualitative approach, the system's risk exposure is reviewed based on its ability to fulfill the three basic goals of security, i.e., system confidentiality, integrity, and availability. The paper is organized as follows: first we account for related work and describe the smart home automation system developed in the research project, which we then apply the risk analysis to. A compilation of the identified risks is then discussed along with three risk scenarios. In the end, conclusions and suggestions for future work are presented.

II. Related Work

As homes are being increasingly computerized and filled with devices ranging from smart TVs to home energy management systems, potential computer security attacks and their impact on residents need to be investigated. Denning et al. [8] survey the security and privacy landscape in IoT-based smart home environments, and provide a strategy for reasoning about security needs. They conclude that the new capabilities of home technologies enable novel attacks and at the same time allow some traditional attacks to have new consequences. There is thus a need for both analyzing and mitigating old, as well as, new risks in smart home automation environments. This is confirmed in the work of Roman et al. [23], where, e.g., an account for threats based on security and privacy perspectives is provided. They also conclude that in IoT scenarios, not only the old threats, but also some new threats must be handled. To manage this, open problems remain in many areas, such as, cryptographic mechanisms, network protocols, data and identity management, user privacy, self-management, and resilient architectures.

Kirkham et al. [16] explore cloud computing in the context of home resource management and propose a risk-based approach to wider data-sharing between the home and its external services using key indicators related to risk, trust, cost, and efficiency. They point out the need for further study on the integration of risk calculation and the expression of risk in the IoT-intense domains; especially in smart home environments inhabited by (human) users, where a lot of potentially sensitive data is in traffic.

In the work by Babar et al. [2], an embedded security framework for IoT environments is proposed. Based on the review of network-based attacks on IoT systems, they investigate the need to provide built-in security in the connected devices to provide a flexible infrastructure for dynamic prevention, detection, diagnosis, isolation, and countermeasures against successful security breaches. Based on this analysis, they define security needs while taking into account computational time, energy consumption, and memory requirements of the connected devices. They also claim that security requirements for IoT will certainly underline the importance of properly formulated, implemented, and enforced security policies throughout their life-cycle. However, in order to achieve this, risk analyses need to be applied to help define and motivate the security requirements.

Gan et al. [11] focus on the application of IoT environments and analyze existing security risks to network points of entry. They conclude that major risks consist of instantiations of malicious software and various hacking techniques, and that they are important threats to mitigate by, e.g., authentication and cryptography between the communicating objects. Although, it is also pointed out that much effort is still needed on further investigations on security design features in infrastructure and system planning, and that this requires a deep understanding of both risk factors and the technology itself.

Regarding security issues of communicating objects in smart home automation, a significant research effort has been undertaken on cryptography tailored for low-cost, low throughput, resource-constraint devices, etc. [18]. This domain has been referred to as "light-weight cryptography", and has produced a number of new protocols that have been proposed for small devices, such as RFID tags. In spite of the large number of available methods, there are very few, which have been examined enough to be considered secure [18].

Weber [25] explored issues of privacy in the IoT model with a special emphasis on judicial perspectives on technical components, such as, encryption, authentication, ID management, etc. He also studied users' rights, public awareness, disclosure statements, and user advocacy. From a legal perspective, Weber [25] analyzed user consent, collection limitation, use limitation, openness, and accountability. He concluded that while according mechanisms still need to be developed, the early recognition of eventual problems and suggestions for their encounter need to be recognized before the IoT can be in full operation.

As mobile devices continue to grow in popularity and functionality, the demand for advanced ubiquitous mobile applications that support home security and surveillance also rises. For instance, Das et al. [7] has designed a home automation and security system (HASec) for mobile devices that leverages IoT technology to provide essential security and associated control functions. In particular, HASec operates and controls motion detectors and video cameras for remote sensing and surveillance, streams live video, records it for future playback, and manages operations on home appliances, such as, turning on/off a TV or microwave, or altering the intensity of lighting around the home.

Analyzing risk exposure is essential in the definition of a proper security strategy for integral information system resources, according to Radomirovic [22]. The application of the ISRA approach, which is one tool to achieve this, has been applied in the context of complex information exchange services in Internet-based collaborative networks (cf. [6]). In a setting, such as, IoT-based smart homes, where applications, devices, and people often collaborate (but not always), it is crucial for the involved actors to be able to rely on one and other. In making such a decision, the analysis of uncertainty serves as the foundation on which that judgment can be based, and it is thus essential that any such approach is transparent, conclusive, and easy to use.

Proper and efficient integration of security in IoT-based smart home systems must be based on sound analysis of risk, i.e., the likeliness of loss [1][21]. In order to enable the identification of a reasonable level of security in smart home automation systems, a methodology that embraces central security concepts like confidentiality, integrity, and availability, but also crucial processes, such as, prevention, detection, and response is thus useful. Successful IoT security strategies apparently also require a holistic approach, and the risk analysis method used in this paper enables such a starting point. In that sense, the chosen method completes the contributions reviewed in this section.

III. SHAS Architecture

In smart home automation, energy services depend on a broad range of hardware and software components for monitoring and controlling an apartment or building [9][12][26]. In this case, these sensors and actuators record and report metrics, such as, water usage, indoor temperature, CO2 levels, and power consumption. Each device runs independently of each other and communicates using a local mesh network; in this case Zigbee (cf. [3][14]) is used with a home gateway acting as the central node. The gateway runs a minimalistic Linux distribution and relays device information to a remote, or cloud, server over the Internet using the XMPP protocol (cf. [13]). In the SHAS architecture (as depicted in Fig. 1), it is important to effectively make use of the resources accessible higher up in the communication chain, as the availability of memory is limited on sensors and actuators. In an attempt to minimize the impact of outgoing Internet traffic, values are only reported from the in-house gateway if they deviate beyond a given threshold. Nevertheless, the gateway also has limited storage and computation capabilities, and in turn offloads data to the cloud server. Prior to this, the gateway also aggregates data over a certain period or within a certain interval.

The cloud server provides the platform with an API entry point that applications use to interact with the apartments in the building through the available devices. The platform API, however, does not grant access directly to the devices for application developers. Instead, the cloud server acknowledges an action to the application immediately and makes the necessary arrangements to ensure that a particular device's state is modified. For example, users wanting to turn off their bedroom lamps use their tablet computer to remotely perform this action. An API-call is then directed to the server over HTTPS, which immediately responds with a reference that the application can use to verify that the desired state was entered. Alternatively, users may switch off the lamps manually. This state change must be propagated via the in-house gateway to the cloud server and, eventually, to applications and services in order to ensure that a consistent view of the device's state can be presented to the user. A representation of the device's state is thus stored at the server and this must be kept consistent by the actual device (as it is the true source).

The data provided through the API is a composition of several data sources, some provided manually by the user, some by external service providers, and obviously some by sensors on the actual device. The user, in turn, assigns contextual information to a connected device, such as, which appliance the smart devices control and where in the apartment they are located. This information is vital for application developers when, e.g., implementing smart shutdown of appliances based on user presence. From an application developer's perspective, the API exposes a composite set of information about devices and the basic services as part of the SHAS. Also, having externally contributed data, as part of the platform API, may unintentionally complicate error handling for the application developer. Furthermore, an API does not provide insight into which devices are available in an apartment only by describing the structure and exposed methods. Device types and their hierarchy must thus be communicated to application developers so that they do not misinterpret which aggregated data is already represented elsewhere.

The SHAS platform used for the connected devices is distributed across multiple hardware solutions, each with its own set of responsibilities and privileges. As the available devices in each apartment differ, each instance of the platform will subsequently be different. There are, however, some components, which are fundamental for the platform's operational capacity, e.g., the in-house gateway for relaying messages that devices send over the local communication protocol (Zigbee or ZWave) to an Internet-based protocol (XMPP). Furthermore, there are devices, which have strong temporal behavior, such as a user's mobile phone, which may be used as a contributor for determining the presence of a particular person, but cannot be guaranteed to always be present (or in itself always valid).

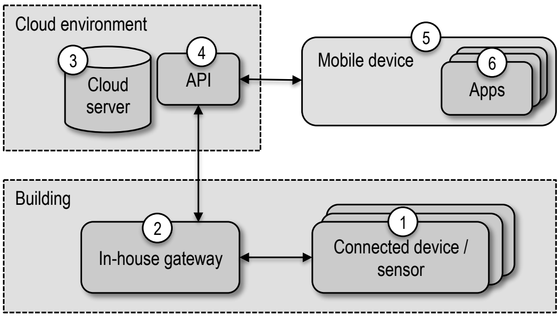

Fig. 1. An architectural view of the SHAS and the link to its physical devices. The numbers refer to the parts of the risk analysis described in IV.

In the current version of SHAS, standard security features, such as, firewall on the cloud server and one-level authentication configuration in the mobile app, are included. However, in order to decide how security should ideally be configured, a risk analysis must be undertaken.

IV. Information Security Risk Analysis

Basically, there are two categories of risk analysis approaches: qualitative and quantitative [21]. As Karabacaka and Sogukpinar [15] point out, quantitative risk analysis methods use mathematical and statistical tools designed to represent risk or risk values in numerical or formal ways. In qualitative risk analysis methods, risk is analyzed with the help of a description of some sort, not primarily based on, e.g., a formal model of probability calculation [1]. Risk analysis methods that use purely quantitative measures may not be suitable in highly connected IoT infrastructures [19], where systems have both a heterogeneous structure, complex relationships of connected devices and deployed software, as well as, a widespread use. However, one important drawback for qualitative risk analysis methods is their nature that may yield inconsistent results. Since qualitative methods are typically not based on mathematics and statistics to model risk exposure, the result of the method is vastly depending on the experience of the people who conduct the risk analysis, which, however; also may be viewed as a merit [21].

In two half-day workshop sessions containing security experts and system developers of the SHAS (described in III), an open questionnaire was used in order to reason, identify, analyze, and evaluate threats, their linkings to system vulnerabilities, as well as, their likeliness of occurrence and potential impact to the entire SHAS. During the workshop sessions each participant individually estimated the corresponding probability and impact associated with each threat based on a five level scale [1-5]. For each threat, the arithmetic mean of both the probability and consequence values was calculated using the input from each participant, rounding it off to an integer if needed. Finally, a mean risk value, within the accessible range [1-25] was calculated for each threat by multiplying the mean probability and consequence values.

In order to reduce complexity in the task, an information system-based approach to analyzing threats, vulnerabilities, and risk levels of the SHAS was applied. The SHAS was consequently viewed in analogy of an information system (cf. [20]), and thus divided into subcategories containing software, hardware, information (or data), communication protocols (including radio communication), and the human actors (whether as end-users or representatives for, e.g., vendors). The analyzed SHAS was divided into the following six parts (which are also mapped to the parts forming the architecture of SHAS, as illustrated in Fig. 1):

1. Connected sensors/devices (S).
2. In-house gateway (GW).
3. Cloud server (CS).
4. API (API).
5. Mobile device (MD).
6. Smartphone apps (App).

Each of the parts above was analyzed in search for vulnerabilities and threats related to hardware, software, information, communication, and human aspects. If a risk was identified, it was given a unique descriptor (identifier) based on the system part and threat group it belonged to. For instance, the second software-related threat (S) concerning the in-house gateway (GW) is denoted S.GW.2, as can be seen in TABLE II.

V. Results

The results of the ISRA applied on the SHAS were analyzed in two phases. In the first phase, a total of 33 potential dangers were identified and analyzed. In the second phase, a prioritization of the most severe threats (representing mean risk values above or equal to 6) based on their potential impact and occurrence was done; resulting in that a more detailed analysis of the remaining 23 risks then took place.

A. *First Phase Risk Factors*

A compilation of the threats identified in phase one is illustrated in TABLE I. where the numbers indicate low (≤5), medium (6-9), or high (≥10) risks in that order. The identified risks are also mapped to both system resources and their corresponding subcategories. Furthermore, each entry in the table shows the number of threats based on their impact levels.

As can be seen in TABLE I. the main source of risk is connected to software components, and especially to the subcategories of apps and API. For the remaining parts, i.e., sensors, cloud servers, in-house gateway, and mobile device, the number of risks is more evenly distributed. It was found that risks derived from the human factor need more careful consideration, as they are inherently complex in nature.

The identified risks were investigated somewhat late in the SHAS development process, i.e., after the integration of a minimum set of standard security-enhancing processes. This circumstance may explain the relatively small amount of high risk levels.

TABLE I. Identified threats based on their impact level Low/Medium/High for the targeted system subcategories.

Id	**Softw.**	**Hardw.**	**Inform.**	**Netw.**	**Human**
S	0/0/0	0/1/0	1/0/0	0/1/0	
GW	0/2/1	0/1/0	0/1/1	0/1/0	
CS	0/1/0	1/0/0	2/0/0	0/1/0	
MD	1/0/0	1/0/0	1/0/0	1/0/0	
App	1/2/1	0/0/0	0/0/0	0/0/0	
API	0/4/0	0/0/0	0/0/0	1/0/0	
Total	2/9/2	2/2/0	4/1/1	2/3/0	0/1/4

B. *Second Phase Risk Factors*

Below, we go through the risks with the highest risk values in each SHAS category, as illustrated in TABLE II. where a description of the 23 risks with an impact level ranging from medium to high can be found. Each row in the table describes a risk factor based on the following four properties:

- The unique identifier previously described.
- A short description of the vulnerability.
- A short description of the threat that exploits the vulnerability.
- A mean risk value, which is the product of multiplying the risk's estimated probability by its consequence.

In the analysis results, the risks connected to hardware mainly concern theft, manipulation, and sabotage of the various devices and servers used within the SHAS. To mitigate these threats, we can conclude that appropriate physical and perimeter security is needed.

Regarding the software risks, S.App.3 concern software vulnerabilities in the SHAS mobile app. Software vulnerabilities are ubiquitous in almost any computer system. They therefore convey the risk of attackers that could exploit these software vulnerabilities. To mitigate such risks, it is important to adopt secure coding practices and rigorous testing techniques, including penetration testing. Furthermore, it might be fruitful to deploy the use of signing the software based on cryptographic certificates and trusted third parties. In the risk S.API.4, the possibility of software vulnerabilities in the API, which could allow attackers to execute unauthorized actions through the API, is highlighted. Although a rather moderate risk value, this can allow for reading and/or modification of information in the SHAS, which, if not attended to, can render the system vulnerable to information collection from multiple sources outside the SHAS.

TABLE II. IDENTIFIED RISKS TARGETING SENSORS (S), THE CLOUD SERVER (CS), THE IN-HOUSE GATEWAY (GW), MOBILE DEVICES (MD), THE API (API), AND SMART PHONE APPS (APP). THE RISK VALUE INDICATES DEGREE OF EXPOSURE; THE HIGHER THE VALUE, THE HIGHER THE RISK.

Id	**Hardware related (H)**		
	Vulnerability description	***Threat description***	***Risk value***
H.GW.1	Lack of physical security policy	Theft, sabotage/destruction, and tampering	7
H.S.1	Inadequate physical security	Theft, sabotage/destruction, and tampering	7
Id	**Software related (S)**		
	Vulnerability description	***Threat description***	***Risk value***
S.GW.1	Irregular deployment of authentication policy (HTTP, SSL)	Unauthorized access to system	8
S.GW.2	Misconfigured event logging policy	Unregistered system events during e.g. attack	10
S.GW.3	N/A since the availability of the service is attacked	Denial of service attacks resulting in loss of service	7
S.App.1	Irregular deployment of authentication policy (HTTP, SSL)	Unauthorized access to system	6
S.App.2	Absense of, or inadequate, access control policy and configuration	Unauthorized modifcation of functions	7
S.App.3	Exploitable software security settings in app	Unauthorized modification of functions	11
S.API.1	Irregular deployment of authentication policy (HTTP, SSL)	Unauthorized access to system	7
S.API.2	Absence of, or inadequate, access control policy and configurations	Unauthorized modification of functions	7
S.API.3	Misconfigured event logging policy	Unregistered system events during, e.g., attack	7
S.API.4	Exploitable software security settings in API	Unauthorized modification of functions	9
S.CS.1	Exploitable software security settings in the cloud environment	Unauthorized modification of functions	6
Id	**Information related (I)**		
	Vulnerability description	***Threat description***	***Risk value***
I.GW.1	Inadequate authentication configuration	Manipulation and disclosure	8
I.GW.2	Absense of, or inadequate access control policy and configuration	Inadequate authenticcation and access control	10
Id	**Network communication related (N)**		
	Vulnerability description	***Threat description***	***Risk value***
N.S.1	Inadequate configuration management of authentication and confidentiality policies	Manipulation and/or disclosure data of transmission	8
N.CS.1	Inadequate authentication and confidentiality protocols	Manipulation and/or disclosure of data transmission	8
N.GW.1	Lack of support for authentication and confidentiality over HTTPS	Manipulation and/or disclosure of transmission	6
Id	**Human related (U)**		
	Vulnerability description	***Threat description***	***Risk value***
U.1	Disgruntled employee including third party contractors	Unauthorized distribution of confidential information	6
U.2	Inexperienced end-users	Various degrees of social engineering attacks	14
U.3	Gullible users	Privacy threats, e.g., commercialization or gamification	11
U.4	Poor password selection	Circumvention of authentication mechanisms	15
U.5	System configuration	Hacking exploration attacks	10

The software risk denoted S.GW.1 entails that the authentication mechanism is vulnerable to attack, allowing attackers to circumvent, e.g., password authentication schemes and thereby gain access to the system without proper credentials. To mitigate this risk, the use of standardized components for handling authentication and session control should be utilized over such components implemented within SHAS. As always, it is important to continuously install software patches released for any software packages used to mitigate these types of risks.

Another software-based risk targeting the in-house gateway is S.GW.2, which represents inadequate accountability and logging settings. If realized, this may render in that system events remain unregistered. This can create severe problems in handling bug fixing, as well as, intrusion attempts. Although this is currently handled in the SHAS, synchronization of logging and registry activities need careful configuration and policy alignment, which of course need to be respected by all included parties.

As is shown in the software risk S.GW.3, the SHAS, like all systems, can be exposed to denial of service attacks due to its inherent property of publishing services, i.e., there is no explicit vulnerability connected to this threat. In SHAS, the configuration of the cloud server can enable flooding of messages to the in-house gateway, rendering in that the SHAS becomes unavailable. This risk can, albeit ubiquitous in any computer system, be mitigated by either deploying in-house equipment from external vendors, or by benefiting from mitigation techniques provided by Internet service providers.

The highest ranked risk related to the information/data processed within the SHAS is I.GW.2, which represents inadequate access control configuration in the in-house gateway. In the current version of the SHAS, there is no access control mechanisms at all implemented since the in-house gateway only can handle a single user account, i.e., the administration user. However, for the future, where multiple user accounts on the in-house gateway will be mandatory, access control settings need to be in place. Another important task, also pointed out in [4], is to allow for temporary access to guest applications, devices, etc.

Within the category of network communication, the highest ranked risks concern inadequate authentication and confidentiality settings within the various connected sensors, as well as, in the remote cloud server. The risk labeled N.S.1 highlights the problem with sensitive information that can be transmitted between the sensors and the in-house gateway, e.g., commands with instructions to switch on/off electronic devices, such as, alarms and surveillance cameras. To mitigate this risk, such information should not typically be sent in clear text, and thus a secure communication (encrypted) protocol is needed in SHAS. In addition to protect against confidentiality threats, the protocol also needs to be able to resist manipulation threats so that the preconditions for replay attacks are minimized.

Furthermore, N.CS.1 highlights the risk concerning inadequate authentication and confidentiality configuration in the network communication between the various subsystems. This problem could be addressed using encryption and authentication schemes that are regulated using legal contracts with the cloud service providers, as this relates to potentially sensitive user data transmission.

In terms of security, human actors represent a weak link in all computer-based information systems. As such, humans constitute a complex challenge to handle in any risk analysis of computer systems, which has proven to be the case also in SHAS. The highest ranked risk concerning human aspects is the deployment of weak passwords (U.4), which could be mitigated through the enforcement of password policies and verification tools. This is especially important in the single user account used within the in-house gateway. Furthermore, user accounts are often – when default configured – a weak point for hacking attempts and man-in-the-middle attacks. It is also important to recognize that the origin of the human-oriented risks span from gullible end-users that usually constitute targets in, e.g., social engineering attacks (U.3) to disgruntled employees that can either sell or deliberately leak confidential information in order to, e.g., make a profit or cause harm or inconvenience to the employer (U.2). The tools available for addressing these threats are usually grouped in policies and legal contracts, as well as, in education efforts of the end-users.

VI. Discussion

In the development of SHAS, software testing in order to identify bugs and other vulnerabilities has been deployed throughout the entire process, which, to some extent, is also the case with security analysis. This circumstance may explain the relatively low number of high risk levels identified in V. Mainly, the most severe risks concern human actors, where mitigating measures rely more on how to inform or train users than to improve the technical design of the SHAS. Also, experience shows that system security needs constant attention in order to prevent, detect, and react to malicious or selfish intrusion or manipulation attempts.

A significant characteristic of smart home automation is that the regulatory controls of the system applications cannot only be managed from ordinary computers, but also from smart phones, tablets, etc. From a security perspective, this means several new contact areas between the system and its potential attackers. One example of a simple, but effective attack is if an end-user enters a security flawed web page that includes malicious software, which exploits a vulnerability in the end-user's computer, smartphone, or tablet. As a result of this, the attacker can execute software on the compromised system, through the malicious software, and by doing so also secretly govern and monitor the SHAS. The only prerequisite for this attack is a user with poorly configured computer equipment, i.e., failing to meet a minimum of standard security features. Statistically, this will be the case for a non-negligible part among the end-users of smart home automation. More advanced examples of this attack could involve various types of social engineering and phishing schemes to lure even more security unaware users into the attack.

Nevertheless, the risk analysis has pointed out some serious flaws in the current system architecture. This is mainly handled by proposing improvements based on experience from similar areas, i.e., using similar techniques with a similar scope. It is likely to believe that application areas with longer and more profound experience are more mature when it comes to security issues, and thus beneficial to learn from. We believe that the system must be designed to address deficiencies in a dynamic way by avoiding cumbersome built-in static security controls, e.g., by supporting programmable and thus adjustable solutions.

A key issue in smart home automation is the users' privacy [24], where the configuration of the system architecture is only one part. As such, it is paramount to take the entire home environment into account in the analysis. Altogether, smart home automation portrays a dynamic, almost unpredictable, future development of IoT systems, which raises the users' stake when it comes to privacy implications. Especially, since smart home automation service providers may be fierce competitors looking for business advantages, e.g., by gaining more information about its customers' energy consumption. As a result, consumers could find themselves in yet another situation where they are expected to emit personal information regarding the activity in their home environment. Such information is typically sensitive and could be misused by actors with antagonistic or selfish intentions that find new opportunities within familiar areas, e.g., related to residential burglary and other types of attacks on the home environment.

It is not possible to entirely predict how the IoT development within smart home automation will progress. However, the following four parameters are important to consider:

1. Security is an ongoing process. Incomplete systems, such as in the case with SHAS, give rise to arms races, i.e., deficiencies will be identified and addressed, which in turn gives rise to new, more advanced attacks and defenses, and so on.
2. Competition between service providers leads to increased collection of end-user related information and increased commercial use. Often, this is not illegal, but rather an expanded "gray area" between smart business ideas and intrusive collection of personal information occurs.
3. There is a ubiquitous risk that a system function is used in a way not intended or that various functions are connected and thereby given new uses or that technology creates new application methods. Each of these aspects could result in additional collection of personal information, which may put user privacy in more ways than anticipated at risk.
4. IoT-connected smart home systems will be integrated with additional applications, stemming also from other environments. In our case, energy supply monitoring may give rise to connections with water supply, garbage facilities, home security services, food shopping, etc. Although, it is quite reasonable that smart home energy management systems, like SHAS, will go in the lead of further development.

Although there are self-evident societal benefits from IoT, smart, connected devices present privacy and security challenges, as well as, opportunities, which require an examination of how traditional privacy norm frameworks like, e.g., the Fair Information Practice Principles[2] should be applied to the smart home automation scenario. Privacy concerns the collection of an individual's data, i.e., stand alone or merged data. As threats generally depend more on the amount of data than on how sensitive it is, questions need to be asked about the distinction between public and private data, how they are handled and who has access to such potentially big, yet sensitive data.

Increasingly, the home is no longer a private closed environment. An important question in this respect concerns where to draw the line between public (or corporate) and personal information. Instead of a static limit, it would be beneficial if users (e.g., as tenants) themselves could in an easy and transparent manner configure the system according to their own privacy preferences. How information is collected, stored, and handled, as well as, what laws, polices, and standards that regulate this is another relevant issue. On this theme, it is of course important to ensure legal compliance given the obvious aspect of (accidental or intentional) privacy breaches. Technical mechanisms regulating access to the collected information, and how such access can be requested are also of great concern. Clear contracts of data sharing and usage are needed in the form of user data management services, proper service level agreements with third party actors, and methods for raising awareness of the possibilities, but also of the risks connected to smart home automation systems.

A. *Scenarios of the Private/Public Home*

As property, as well as, users and the information that they are generating constitute an integral part of smart home automation, it is crucial to analyze not only the system risks related to privacy and security, but also the type of scenarios that they entail. Below, we illustrate three such examples.

1) *Surveillance Camera Use*

In smart homes, the use of a surveillance camera typically has a purpose to detect anomalies in the home environments. Examples of anomalies can be, e.g., the detection of fire, the documentation (and prevention) of burglaries, or involve detection of other unexpected events, such as, water leaks, etc. The surveillance camera can also be used in more benign purposes, such as, to see who is at home (including child care, control of infants sleeping, etc.) or review performance statuses, e.g., if lamps are switched on or off, doors closed or open, etc. Smart home surveillance cameras can be used in combination with motion detectors, and other sorts of connected devices. In addition, surveillance cameras typically raise the need for increased security restrictions, especially in terms of features enabling remote access to home cameras possibly involving persons in their private state (cf. [4]).

2) *System Function Linkings*

Different system functions, including the data they are handling, linked together can provide an undesirable level of knowledge about the residents of a home. Measuring the overall power consumption provides a limited knowledge of the home, but the addition of electrical sources measurements (usage extent, time of day, etc.) can provide meta information about a family members' habits. All such digital traces that the users (more or less voluntarily) leave behind when using the system can build extensive personal profiles of the residents of a home, e.g., routine activity patterns based on when persons in the household are at home. It could also be possible to create estimates about the activities the household members are involved in based on different usage of electrical devices that leave distinct signatures. This type of information is sensitive, for instance, in the sense that there is a risk for misuse with severe consequences, such as, unsolicited commercial message exposure, stalking situations, etc. There is of course also a conflict between the service providers and consumers; the former want to collect as much information as possible for future reference or business opportunity, while consumers primarily only want to reveal small pieces of information that is useful at a certain point in time. However, it is important to investigate what actual choice the customers are faced with regarding participation in the data collection process. If there is a choice for the customer to make, i.e., the installation of the smart home automation system is not a mandatory policy by the supplier/vendor, then additional methods for increasing the system transparency in terms of user data management and storage towards the customer is needed. Also, this puts accentuated requirements on the technical security configuration of the system architecture.

3) *Security Support*

A possible new application in smart home automation is to use energy control to prevent burglary, for instance, when the home is unoccupied for long periods. This is an extension of scheduling the lights to include also other types of electronic connections, such as, Internet-connected radio, TV, and other types of consumer electronic equipment. This is of course the opposite to making sure all power is off, and thus may contribute little to the idea of energy efficiency. However, the scheduling of more electrical devices in homes may convince potential burglars to avoid breaking entries, as they may be lured into thinking that the home is in fact occupied. Moreover, by using energy control appliances in such a way, another drawback may be that the home can become vulnerable to the threats and intrusion attempts that are usually associated with online connections, rendering an extension of security analysis to also include situations where no actual (human) user is around, but where the user unexpectedly may play an important part in the resilience and security configuration of smart homes.

VII. CONCLUSIONS AND FUTURE WORK

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 that combines various vendors' systems has been developed. Using this common interface, third party stakeholders can both monitor energy consumption and remotely control electronic devices in the homes and buildings. Open system architecture allows end-users to access various applications through an ecosystem of online services and smartphone applications. In this highly connected and complex environment, a risk analysis set to identify the most severe potential dangers has been undertaken.

One of the main sources of risk is connected to the software components, and especially in the mobile apps and APIs. The risks to hardware concern theft, manipulation, and sabotage of the various devices and servers used within the SHAS, also

[2] Cf. the following URL: http://www.nist.gov/nstic/NSTIC-FIPPs.pdf Last checked 2014-04-02.

need careful attention. The highest ranked risk related to the information/data processed is derived from inadequate access control configuration in the in-house gateway. Within network communication, the main risks come from inadequate authentication and confidentiality settings. The most severe risk confirmed in the risk analysis, is the human factor, i.e., as such, humans represent the highest risk exposure in smart home automation systems.

In three risk scenarios of a smart home automation system, it has been discussed that connected devices may cause undesirable results with respect to, e.g., surveillance camera control, access to potentially sensitive meta information, and the misuse of user-intense mobile devices, e.g., smart phones. The most sensitive part of smart home automation systems concern information registry about the users' energy consumption, from which conclusions about people's daily routines, life situations, etc., can be drawn, which may form decision support for criminal activities, such as, e.g., burglary and stalking.

All computer systems may leak information, if not through the vulnerabilities and soft-/hardware configurations, or selfish or malicious acts, so through human error. Bearing in mind that questions need to be asked about the distinction between public and private data, how they are handled, and who has access to sensitive data; the primary challenge is to combine business strategy for the vendors with a reasonable level of privacy assurance for the users, while at the same time meeting necessary security requirements.

For future work, a separation between threats affecting a single user and the entire system should be conducted, i.e., the latter one being the more important challenge to take on in order to produce a holistic system view. This is particularly important with respect to the challenges related to human actors, as these do not rely on standard security features alone. Furthermore, end-users need increased transparency with regards to the information collection and use within the system. As such, an investigation in existing smart home automation techniques for increasing transparency towards the end-users would be feasible.

Acknowledgment

This work has been carried out within the project "Mobile Services for Energy Efficiency in Existing Buildings", partially funded by Vinnova – the Swedish Governmental Agency for Innovation Systems. The authors would also like to thank all the members of the project.

References

[1] J. Adams, Risk, Oxford: Routledge, 2000.

[2] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed Embedded Security Framework for Internet of Things (IoT)", Int. Conf. on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2011.

[3] P. Baronti, P. Pillai, S. Chessa, A. Gotta, and, Y.F. Hu, "Wireless Sensor Networks: A Survey on the State of the Art and the 802.15.4 and ZigBee Standards", Computer Communications, Vol. 30, Issue 7, 2007.

[4] A.J. Bernheim Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon, "Home Automation in the Wild: Challenges and Opportunities", Proc. of the ACM CHI Conference on Human Factors in Computing Systems, 2011.

[5] S. Björnehaag, "Test of a Home Energy Management System at E.ON – an Evalutaion of Users's Expectations and Experience", Master Thesis, Dept. of Energy Sciences, Lund University, 2012.

[6] B. Carlsson, P. Davidsson, A. Jacobsson, S.J. Johansson, and J.A. Persson, "Security Aspects on Inter-Organizational Cooperation Using Wrapper Agents", Agent-Based Technologies and Applications for Enterprise Interoperability, Lecture Notes in Business Information Processing, Vol. 25, pp. 220-233, Berlin: Springer, 2009.

[7] S.R. Das, S. Chita, N. Peterson, B.A. Shirazi, and M. Bhadkamkar, "Home Automation and Security for Mobile Devices", IEEE Int. Conf. on Pervasive Communities and Service Clouds, 2011.

[8] T. Denning, T. Kohno, and H.M. Levy, "Computer Security and the Modern Home", Comm. of the ACM, Vol. 56, No. 1, pp. 94-103, 2013.

[9] U. Eklund, C.M. Olsson, and M. Ljungblad, "Characterising Software Platforms from an Architectural Perspective", Software Architecture, Lecture Notes in Computer Science, Vol. 7957, pp. 344-347, Berlin: Springer, 2013.

[10] A. Fensel, V. Kumar, and S.D.K. Tomic, "End-User Interfaces for Energy-Efficient Semantically Enabled Smart Homes", Energy Efficiency, Springer-Business Mediea, Dordrecht: Springer, 2014.

[11] G. Gan, Z. Lu, and J Jiang, "Internet of Things Security Analysis", IEEE Conf. on Internet Technology and Applications, 2011.

[12] D.M Han and J.H. Lim, "Design and Implementation of Smart Home Energy Management Systems based on ZigBee", IEEE Trans. on Consumer Electronics, Vol.56 , Issue: 3, pp. 1417-1425, 2010.

[13] A. Hornsby, P. Belimpasakis, and I. Defee, "XMPP-Based Wireless Sensor Network and its Integration into the Extended Home Environment", IEEE 13th Int. Symp. on Consumer Electronics, 2009.

[14] A. Kailas, V. Cecchi, and A. Mukherjee, "A Survey of Communications and Networking Technologies for Energy Management in Buildings and Home Automation", Journal of Computer Networks and Communications, Vol. 2012, Article ID 932181, 12 pages, 2012.

[15] B. Karabacaka and I. Sogukpinar, "ISRAM: Information Security Risk Analysis Method", Computers and Security, 24(2), pp. 147-159, 2004.

[16] T. Kirkham, D. Armstrong, K. Djermame, and M. Jiang, "Risk Driven Smart Home Resource Management Using Cloud Services", Future Generation Computer Systems, Elsevier, 2013.

[17] T. Kowatsch and W. Maass, "Critical Privacy Factors of Internet of Things Services: An Empirical Investigation with Domain Experts", Knowledge and Technologies in Innovative Information Systems, Lecture Notes in Business Information Processing, Vol. 129, pp. 200-211, Dordrecht: Springer, 2012.

[18] R. van Kranenburg, E. Anzelmo, A. Bassi, D. Caprio, S. Dodson, and M. Ratto, "The Internet of Things", Proc. of the First Berlin Symposium on Internet and Society, 2011.

[19] N. Shukla and S. Kumar, "A Comparative Study on Information Security Risk Analysis Practices", IJCA Special Issue on Issues and Challenges in Networking, Intelligence and Computing Technologies ICNICT(3), pp. 28-33, 2012.

[20] J. O'Brien and G. Marakas, Management Information Systems, 10ed., New York: McGraw-Hill, 2010.

[21] T.R. Peltier, Information Security Risk Analysis, Boca Raton: Auerbach Publications, 2010.

[22] S. Radomirovic, "Towards a Model for Security and Privacy in the Internet of Things", Proc. First Int'l Workshop on Security of the Internet of Things, 2010.

[23] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things", IEEE Computer, vol. 44, no. 9, pp. 51-58, 2011.

[24] M. Rozenfeld, "The Value of Privacy – Safeguarding Your Information in the Age of the Internet of Everything", The Institute, IEEE, March 7, 2014.

[25] R. Weber, "Accountability in the Internet of Things", Computer Law & Security Review. Vol 27, pp. 133-138, 2011.

[26] S.H. Yuang, "ZigBee Smart Home Automation Systems", Wireless Sensor Networks: Principles, Design and Applications, pp. 263-274, London: Springer, 2014.